> **This version of GitHub Enterprise Server was discontinued on 2026-04-09.** No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise Server. For help with the upgrade, contact GitHub Enterprise support.

Enterprise Server 3.14 release notes

Enterprise Server 3.14.26

Download GitHub Enterprise Server 3.14.26

April 21, 2026

📣 This is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.26: Security fixes

- **HIGH**: An attacker could gain unauthorized access to private repositories by abusing scoped user-to-server (`ghu_`) tokens after their associated GitHub App installation was revoked or deleted. In certain cases, the authorization layer could incorrectly fall back to a global installation context instead of rejecting the request, allowing the token to access resources outside its intended installation or repository scope. This issue could be chained with weaknesses in token revocation timing and SSH push attribution to obtain a victim-scoped token and read private repository contents without victim interaction. GitHub has requested CVE ID CVE-2026-5845 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker could extract sensitive environment variables from a GitHub Enterprise Server instance through a timing side-channel attack against the notebook rendering service. When private mode was disabled, the notebook viewer followed HTTP redirects without revalidating the destination host, enabling an unauthenticated Server-Side Request Forgery (SSRF) to internal services. By measuring response time differences, an attacker could infer secret values character by character. GitHub has requested CVE ID CVE-2026-5921 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **HIGH**: A Management Console administrator could inject shell metacharacters into configuration fields via the Management Console configuration API, leading to arbitrary command execution on the appliance as the admin OS user. GitHub has requested CVE ID CVE-2026-4821 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker with knowledge of a target application's registered OAuth callback URL could gain unauthorized access to user accounts by exploiting incorrect regular expression matching in callback URL validation. GitHub has requested CVE ID CVE-2026-4296 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An attacker with permission to manage secret scanning push protection settings in one repository could add or remove delegated bypass reviewers in a different repository by exploiting an incorrect authorization check in the `/settings/security_analysis/bypass_reviewers` endpoints. Authorization was checked against the repository in the URL route, but the action was applied to a different repository specified in the request body. The impact is limited to assigning existing trusted users as bypass reviewers. GitHub has requested CVE ID CVE-2026-3307 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An authenticated attacker could determine the names of private repositories by their numeric ID through the mobile upload policy API endpoint, which returned repository names in validation error messages without verifying the caller's access. GitHub has requested CVE ID CVE-2026-5512 for this vulnerability, which was reported via the GitHub Bug Bounty program.

3.14.26: Bug fixes

- On an instance with GitHub Actions enabled, diagnostic log files for storage connectivity checks did not persist to disk when site administrators clicked **Test storage settings** in the Management Console or ran `ghe-config-apply` to apply configuration changes. This made storage connection failures difficult to troubleshoot because logs were unavailable in support bundles.
- When Consul replication failed to start, a misleading error message `exit: check_consul_replication: numeric argument required` was emitted to `ghe-config.log`.
- Consul replication would sometimes fail to start and would repeatedly display an error message `WARNING: Consul KV Replication Error` before terminating.
- On instances with Dependabot enabled, hotpatch upgrades could lock the Nomad jobs queue.
- The site admin bar displayed debugging information used by GitHub.

- On an instance with busy databases, online schema migrations using gh-ost failed because the cut-over lock timeout defaulted to 3 seconds, which was insufficient to acquire an exclusive table lock under continuous traffic.

3.14.26: Known issues

- First time setups of GitHub Actions with OpenID Connect (OIDC) fail with an error on the `Update Servicing Resources` step. This problem does not affect instances where GitHub Actions is already enabled.

  As a workaround, you can enable Actions without OIDC, then enable OIDC **immediately** once the process completes. You should do this immediately because enabling OIDC will remove all access to existing Actions logs and artifacts.

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.

- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.

- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.

- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.

- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.

- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.

- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git

operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.

- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.

- GitHub Enterprise Server releases shipped with mismatched Git versions between containers.

Enterprise Server 3.14.25

Download GitHub Enterprise Server 3.14.25

March 12, 2026

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.25: Security fixes

- **HIGH**: An attacker with push access to a repository could execute arbitrary code on the instance by injecting malicious values into Git push options. The push options were not properly sanitized before being included in internal headers used for Git operations, allowing the attacker to override internal metadata fields and achieve remote code execution. GitHub has requested CVE ID CVE-2026-3854 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An attacker with read access to a repository and write access to a project could bypass repository write permissions to modify issue and pull request labels, assignees, and other metadata by adding duplicate items to the project. GitHub has requested CVE ID CVE-2026-3306 for this vulnerability, which was reported via the GitHub Bug Bounty program.

3.14.25: Bug fixes

- The Git version included in the release did not match the version used by the gitrpcd service due to incorrect version determination during the build process.
- Users experienced delays or failures when performing Git operations over HTTP. The operations could hang indefinitely due to a deadlock in the babeld service.
- When administrators applied configuration changes via the Management Console, the state shown would occasionally briefly flicker to a failure before being marked as successful causing confusion as to whether the configuration had succeeded.
- After an upgrade, `ghe-config-apply` could fail to remove some pre-upgrade Docker images and report `Error response from daemon: conflict: unable to delete <id>`.
- Administrators for instances using the collectd metrics stack saw empty `git fetch caching` graphs on the Management Console monitoring page.
- After upgrading, `ghe-config-apply` failed to start services including HAProxy and Redis. Docker images were incorrectly removed during the upgrade process, preventing services from starting.
- Users experienced failures when migrating repositories with releases using GitHub Enterprise Importer. Migrations failed to import release assets that were incompletely uploaded at the time of export, as the export archive referenced assets without including the corresponding files.

3.14.25: Changes

- To improve performance on large instances, HAProxy automatically scales its thread count based on available CPUs and uses higher connection limits for high-traffic backend services including GitHub Actions, database connections, job queues, and package registry. Administrators can override the thread count using `ghe-config haproxy-nbthread` if needed.

3.14.25: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. See Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may time out on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running `ghe-config-apply` as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.

- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the Actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.
- On an instance hosted on Azure, commenting on an issue via email means the comment is not added to the issue.

Enterprise Server 3.14.24

Download GitHub Enterprise Server 3.14.24

March 10, 2026

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

> **Warning**: GitHub Enterprise Server 3.14.24 has been unpublished due to mismatched Git versions between containers. Please use the most recent available patch release of 3.14. [Updated: 2026-03-13]

3.14.24: Security fixes

- **HIGH**: An attacker with push access to a repository could execute arbitrary code on the instance by injecting malicious values into Git push options. The push options were not properly sanitized before being included in internal headers used for Git operations, allowing the attacker to override internal metadata fields and achieve remote code execution. GitHub has requested CVE ID CVE-2026-3854 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An attacker with read access to a repository and write access to a project could bypass repository write permissions to modify issue and pull request labels, assignees, and other metadata by adding duplicate items to the project. GitHub has requested CVE ID CVE-2026-3306 for this vulnerability, which was reported via the GitHub Bug Bounty program.

3.14.24: Bug fixes

- Users experienced delays or failures when performing Git operations over HTTP. The operations could hang indefinitely due to a deadlock in the babeld service.
- When administrators applied configuration changes via the Management Console, the state shown would occasionally briefly flicker to a failure before being marked as successful causing confusion as to whether the configuration had succeeded.
- After an upgrade, `ghe-config-apply` could fail to remove some pre-upgrade Docker images and report `Error response from daemon: conflict: unable to delete <id>`.
- Administrators for instances using the collectd metrics stack saw empty `git fetch caching` graphs on the Management Console monitoring page.
- After upgrading, `ghe-config-apply` failed to start services including HAProxy and Redis. Docker images were incorrectly removed during the upgrade process, preventing services from starting.
- Users experienced failures when migrating repositories with releases using GitHub Enterprise Importer. Migrations failed to import release assets that were incompletely uploaded at the time of export, as the export archive referenced assets without including the corresponding files.

3.14.24: Changes

- To improve performance on large instances, HAProxy automatically scales its thread count based on available CPUs and uses higher connection limits for high-traffic backend services

including GitHub Actions, database connections, job queues, and package registry. Administrators can override the thread count using `ghe-config haproxy-nbthread` if needed.

3.14.24: Known issues

- The Git version included in the release did not match the version used by the gitrpcd service due to incorrect version determination during the build process. [Updated: 2026-03-13]
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. See Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may time out on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running `ghe-config-apply` as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.

- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the Actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.
- On an instance hosted on Azure, commenting on an issue via email means the comment is not added to the issue.

Enterprise Server 3.14.23

Download GitHub Enterprise Server 3.14.23

February 10, 2026

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.23: Security fixes

- **MEDIUM:** By supplying the migration identifier, an attacker could upload unauthorized content to another user’s repository migration export due to a missing authorization check. This could cause victims to download attacker-controlled migration archives, potentially impacting the

integrity of downstream repository imports. GitHub has requested a CVE ID CVE-2026-1355 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **HIGH:** An authenticated attacker could exploit a URL redirection vulnerability in GitHub Enterprise Server to leak privileged authorization tokens by redirecting requests to an attacker-controlled domain. This could allow exfiltration of the `Actions.ManageOrgs` JWT and potential remote code execution. This vulnerability was reported via the GitHub Bug Bounty program.

3.14.23: Bug fixes

- Running `ghe-config-apply` could fail if Redis experienced transient connectivity issues during the configuration process.
- On an instance configured behind a load balancer, users received unexpected secondary rate limit warnings during authentication when the `X-Forwarded-For` header included port numbers. This occurred because the system incorrectly ignored the header values containing ports, preventing proper client IP address identification.
- On instances with GitHub Actions enabled, Actions workflow runs could be silently skipped when creating many issues rapidly via the API. Previously, some "issue opened" webhooks were processed before the new issue was saved to the database, causing the event to be dropped and the workflow to not start. After this fix, workflow runs start reliably for all rapid issue creations, regardless of timing.
- Users could only view webhook deliveries from the previous three days.

3.14.23: Changes

- Administrators can configure database connection pool limits for the authentication and authorization services to improve performance on instances experiencing high concurrent request volumes. The limits can be adjusted using `ghe-config` keys: `app.authnd.mysql-max-open-conns`, `app.authnd.mysql-max-idle-conns`, `app.authzd.db-resolver-max-open-conns`, and `app.authzd.db-resolver-max-idle-conns`. The default values remain unchanged (authnd: 100 max open and 100 max idle connections; authzd: 100 max open and 15 max idle connections). These settings should only be adjusted with guidance from GitHub Support.

3.14.23: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.

- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.

- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.22

Download GitHub Enterprise Server 3.14.22

January 06, 2026

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.22: Security fixes

- **HIGH:** An authenticated attacker with permission to configure webhooks could perform SSRF to access internal-only services on the instance, potentially disrupting background job processing. Exploitation required webhook configuration privileges and the ability to craft valid service requests. GitHub has requested CVE ID CVE-2026-1999 for this vulnerability, which was reported via the GitHub Bug Bounty program.

3.14.22: Bug fixes

- On instances with GitHub Actions enabled, when administrators deleted a self-hosted runner from the service, the runner process continued running on the host and did not exit automatically.
- Input validation wasnt correctly being applied to the "Password and authentication policies" section on the Management Console, allowing administrators to specify invalid values for "Login attempt limit for all users" and "Lockout time for Management Console users".

- The highlighted section on the sidebar of the Management Console settings page would not always accurately show what content was currently scrolled into view for an administrator.
- Site administrators could not easily identify when a configuration run for their instance failed in the Management Console. Failed runs were indicated only by a header and steps could remain in a "pending" state.
- Administrators who set the `ELASTOMER_INDEX_LOCK_BACKOFF_ATTEMPTS` environment variable to configure Elasticsearch index lock backoff attempts saw no effect, as the instance required the `ENTERPRISE_` prefix for this variable.
- Commit authors who ignored notifications from a repository did not receive secret scanning alert emails when their credentials were detected in that repository.

3.14.22: Changes

- Administrators can capture distributed tracing data for Nomad job allocations using the `usr/local/share/enterprise/ghe-capture-trace-data` command to help diagnose performance issues. This feature is available only on standalone instances and should be run with guidance from GitHub Support.

3.14.22: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may time out on appliances with many users or repositories. Retrying the request until data is returned is advised.

- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shut down the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository page for locked repositories.

Enterprise Server 3.14.21

Download GitHub Enterprise Server 3.14.21

December 09, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.21: Security fixes

- **HIGH:** An attacker could inject HTML elements with IDs that collided with server-initialized data islands due to insufficient sanitization. When a privileged user viewed crafted content in certain Project views, these injected elements could overwrite critical application state objects, resulting in unintended server-side POST requests or other unauthorized backend interactions. GitHub has requested CVE ID CVE-2025-14046 for this vulnerability, which was reported via the GitHub Bug Bounty program.

3.14.21: Bug fixes

- Due to a regression in a recent patch release, Dependabot did not respond to some commands on pull requests, such as rebases, because webhook deliveries to loopback addresses were blocked. Webhook deliveries to the Dependabot endpoint now succeed, although deliveries to other endpoints on loopback addresses are still blocked.

3.14.21: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see "Troubleshooting access to the Management Console."
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.

- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.20

Download GitHub Enterprise Server 3.14.20

December 02, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.20: Security fixes

- **HIGH:** An attacker could execute code within a victim's browser, potentially accessing sensitive information, by causing malicious HTML to be injected into the DOM when content is rendered by the Filter component found across GitHub. GitHub has requested CVE ID CVE-2025-13744 for this vulnerability, which was reported via the GitHub Bug Bounty program. [Updated: 2026-01-06]
- **HIGH:** A privilege escalation vulnerability was identified in GitHub Enterprise Server that allowed an authenticated Enterprise admin to gain root SSH access to the appliance by exploiting a symlink escape in pre-receive hook environments. By crafting a malicious repository and environment, an attacker could replace system binaries during hook cleanup and execute a payload that adds their own SSH key to the root user's authorized keys—thereby granting themselves root SSH access to the server. To exploit this vulnerability, the attacker needed to have enterprise admin privileges. This vulnerability has been assigned CVE-2025-11578 and was reported through the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

3.14.20: Bug fixes

- Administrators may have experienced delays with configuration runs after a reboot if `ghe-reconfigure.service` was still activating, impacting run performance and stability.
- On instances with a "No Proxy" setting configured for GitHub Actions with MinIO or AWS remote blob providers, administrators sometimes experienced failures reading or writing Actions logs, artifacts, or caches because some traffic was incorrectly routed through the instance's proxy.
- New Microsoft Teams integrations failed to set up because the required `tenant_id` field was missing from the configuration, following Microsoft's deprecation of multi-tenant bot creation.
- An "Invite member" button intended only for GitHub.com was displayed on the enterprise "People" tab.

- Audit log searches could temporarily miss recent events or show incomplete results right after new index creation at the start of a month. Administrators now experience reduced lag between the creation of monthly audit log search indexes and their availability for searches and write operations.
- When new Elasticsearch indexes were created, index routing memos could go to a read-only MySQL replica and fail, causing delays in audit log indexing after monthly rollovers. The memos are now written to the primary database rather than a read-only replica.

3.14.20: Changes

- A new weekly job automatically disables Elasticsearch deprecation logging and removes existing deprecation logs every Saturday at midnight. This helps administrators manage disk space by regularly cleaning up deprecation data streams and log indices that are no longer needed.
- Administrators can add security key-backed (SK) SSH certificate authorities.
- Administrators and users experience faster and more efficient searching of GitHub Actions workflow runs, with lower compute and networking resource usage. Searches for workflow runs within a repository are now always scoped to an associated repository.
- `ghe-repl-start` can now be executed without requiring a maintenance window when setting up a new replica, as long as `ghe-repl-setup` is immediately followed by `ghe-config-apply`. [Updated: 2025-12-17]

3.14.20: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. See "Troubleshooting access to the Management Console."
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.

- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the Actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.

Enterprise Server 3.14.19

Download GitHub Enterprise Server 3.14.19

November 10, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.19: Security fixes

- **CRITICAL:** Redis has been upgraded to version 6.2.20 to address CVE-2025-49844 (also known as RediShell). Administrators should apply this update promptly to mitigate potential security risks.
- **HIGH:** An attacker could execute arbitrary code in the context of other users' browsers by supplying a malicious `label:` value that was injected into the DOM without proper sanitization. This could be triggered when a user visits a crafted Issues search URL, enabling session hijacking, account takeover, and recovery code exfiltration. GitHub has requested CVE ID CVE-2025-11892 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

3.14.19: Bug fixes

- Users applying a new license file received an HTTP 500 error.
- SVG files stored in Git Large File Storage (LFS) failed to render on the web interface.
- On the "Scheduled workflows" page in the site admin dashboard, actors attributed to workflows appeared as "Not found".

3.14.19: Changes

- Elasticsearch deprecation warnings, which are logged to index files in new versions of Elasticsearch, have been disabled. These warnings provided no value to administrators, and in some cases could block upgrades of instances in high-availability or cluster configurations.

3.14.19: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shut down the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. You can also trigger the reindexing by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.

- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.

Enterprise Server 3.14.18

Download GitHub Enterprise Server 3.14.18

September 09, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.18: Security fixes

- Packages have been updated to the latest security versions.

3.14.18: Bug fixes

- When generating a support bundle, site administrators could encounter errors if character escaping caused the bundle script to omit the URL parameter for `curl`.
- In some environments, `syslog-ng` could write excessive logs to a regular file named `tty10`, continuously filling disk space.
- Secret scanning backfills for pull requests and discussions did not run as expected during backfills of new secret types. Site administrators and security teams may have noticed incomplete secret scanning coverage or unworked queues after upgrading.

- Administrators saw daily `SignalException` errors in `github-stream-processors` when log rotation happened. Log rotation using "copytruncate" no longer sends SIGUSR1, preventing these errors and improving log management stability. No administrator action is required.
- Maintenance periods scheduled more than a week in advance were triggered on the first occurrence of the scheduled day-of-week rather than the intended specific date.

3.14.18: Changes

- For administrators managing logs, log folders are more consistently accessible from the administrative account without the need to use `sudo`.

3.14.18: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.

- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.17

Download GitHub Enterprise Server 3.14.17

August 25, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.17: Security fixes

- **HIGH:** An improper access control vulnerability was identified in GitHub Enterprise Server that allowed users with access to any repository to retrieve limited code content from another repository by creating a diff between the repositories. To exploit this vulnerability, an attacker needed to know the name of a private repository along with its branches, tags, or commit SHAs that they could use to trigger compare/diff functionality and retrieve limited code without proper authorization. This vulnerability has been assigned CVE-2025-8447 and was reported through the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.
- Elasticsearch packages have been updated to the 8.18.0 security version.

3.14.17: Bug fixes

- After enabling GitHub Actions or performing an upgrade with GitHub Actions enabled, administrators experienced a delay of approximately 10 minutes longer than they should have due to a faulty connection check. This is fixed for future enablement and upgrades.
- After upgrading to GHES 3.14.16, GHES 3.15.11, GHES 3.16.7, or GHES 3.17.4, administrators found that draft pull requests and autolink references for private repositories were no longer available. [Updated: 2025-11-11]

3.14.17: Changes

- When administrators run the `ghe-support-bundle` command on an unconfigured node, the output clearly states that metadata collection was skipped, instead of producing misleading `curl` errors. This improves the clarity of support bundle diagnostics.

3.14.17: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the

administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) may fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running `ghe-cluster-config-apply` as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.

- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.

Enterprise Server 3.14.16

Download GitHub Enterprise Server 3.14.16

July 29, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.16: Security fixes

- Packages have been updated to the latest security versions.

3.14.16: Bug fixes

- Administrators would occasionally encounter timeouts when downloading diagnostics via the Management Console.
- In full cluster topologies, some expensive stats queries are skipped during `ghe-cluster-support-bundle` to prevent overloading the nodes with identical requests.
- Unsuccessful attempts to sign in to the Management Console were reported in the audit log and were indistinguishable from successful attempts.

3.14.16: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.

- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.

- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.
- The autolink references feature is missing from the repository settings page.
- When attempting to open a pull request as a draft in a private or internal repository, users are incorrectly prompted to upgrade their plan.[Updated: 2025-08-11]

Enterprise Server 3.14.15

Download GitHub Enterprise Server 3.14.15

July 15, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.15: Security fixes

- **HIGH**: An incorrect authorization vulnerability allowed unauthorized read access to the contents of internal repositories for contractor accounts when the Contractors API feature was enabled. The Contractors API is a rarely-enabled feature in private preview. Following this fix, contractor account access to internal repositories via the API will be correctly blocked unless they have an alternate grant. GitHub has requested CVE ID CVE-2025-6981 for this vulnerability.
- Packages have been updated to the latest security versions.

3.14.15: Bug fixes

- Applying a new GitHub Enterprise Server license using the Management Console would sometimes fail with a HTTP 500 error.

- During Git push operations in a HA configuration, it was possible under rare circumstances for the primary voting replica of a repository to become incorrectly marked as out of sync with the other replicas and in need of repair, causing the repository to become unavailable.

3.14.15: Changes

- Site administrators can now set `innodb_buffer_pool_size` in megabytes for MySQL using `ghe-config mysql.innodb-buffer-pool-size VALUE`.

3.14.15: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.

- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.14

Download GitHub Enterprise Server 3.14.14

July 01, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.14: Security fixes

- Packages have been updated to the latest security versions.

3.14.14: Bug fixes

- The Management Console would become unresponsive when saving settings after a failed config apply run.
- Users sometimes received a JSON response instead of a web page when clicking "Back" after viewing files in raw format.
- Pull requests were blocked from merging due to unhandled merge attempt timeouts.
- Pull requests were temporarily blocked from merging due to delayed purging of failed background jobs.

3.14.14: Changes

- The babeld service no longer reports log messages about some common client-induced networking errors, reducing noise in the logs.

3.14.14: Known issues

- Applying a new GitHub Enterprise Server license using the Management Console can sometimes fail with an HTTP 500 error.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.

- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.13

Download GitHub Enterprise Server 3.14.13

June 18, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.13: Security fixes

- **HIGH:** An attacker could execute arbitrary code, potentially leading to privilege escalation and system compromise, by exploiting the pre-receive hook functionality to bind to dynamically allocated ports that become temporarily available (for example, during a hot patch upgrade). This vulnerability is only exploitable under specific operational conditions, such as during the hot patching process, and requires either site administrator permissions or a user with privileges to modify repositories containing pre-receive hooks. The initial fix for this issue was found to be incomplete, leaving the vulnerability exploitable in some cases. GitHub has requested CVE ID: CVE-2025-3509 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

3.14.13: Bug fixes

- On an instance with GitHub Actions configured to connect to Azure OIDC storage through a proxy, Actions logs and artifacts would not be properly stored.
- Site administrators and auditors reviewing audit logs saw the `mc_actor` field was empty when a user signed out, because audit logging occurred after the user was removed from session state.
- During hotpatching, site administrators could encounter issues with the kernel partition table not updating correctly when running `ghe-partition-setup`. These users had to manually intervene in order to complete the upgrade process.
- Users of GitHub Actions could not view or manage Actions artifacts and logs if the global AWS STS endpoint was unavailable, because Actions did not use the configured regional STS endpoint.
- On instances with a large number of code scanning users, running `ghe-config-apply` previously resulted in slow performance.

- Organization owners had no audit log events to track organization announcements displayed on banners in the UI.
- If an Enterprise Managed User (EMU) pushed to their personal repository with both secret scanning and push protection enabled, the custom patterns defined at enterprise level were not being applied during the push protection scan.
- In some situations, the kafka-lite service could cause client timeouts when processing consumer group membership sessions and expirations. [Updated: 2025-07-14]

3.14.13: Changes

- Site administrators can now set rate limits for the WebSockets controller used for live updates, with `ghe-config app.github.web-sockets-rate-limit`. For more information, see Controlling the rate for the live update service.

3.14.13: Closing down

- Site administrators who manage dependencies with the base-pinned image should no longer rely on the vulcanizer CLI, as it is in the process of being retired and replaced with vulcancli. Transition to vulcancli to ensure continued support and compatibility.

3.14.13: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.

- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.12

Download GitHub Enterprise Server 3.14.12

May 27, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.12: Security fixes

- **MEDIUM:** An attacker could inject HTML in the instances web UI because the web commit dialog did not properly sanitize repository rule violation messages. This vulnerability was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

3.14.12: Bug fixes

- Ephemeral runner registrations for GitHub Actions were not fully cleaned up after deletion.
- The alive process intermittently experienced segmentation faults (SIGSEGV) due to a `panic: runtime error: invalid memory address or nil pointer dereference` in the alive daemon during restore operations. These crashes caused services, such as mps, to appear unhealthy, leading to restore operation failures after 20 attempts.
- For instances in a high availability configuration, because there was no Nomad job for the `aqueduct-lite` service on replica nodes, generating a support bundle from the command line on a replica would result in the error `ERROR: Failed to get elastomer index build progress` being incorrectly reported.
- A pre-receive hook could fail due to blocked system calls.
- After updating the TLS certificate from the Management Console, users encountered 502 errors when creating releases and uploading artifacts. Running `ghe-config-apply` did not resolve the issue, as the alambic service required a manual restart.
- The sidebar menu did not display on the "Retired namespaces" page on the site admin dashboard.
- Site administrators could encounter a failure to load domain entries in the "Verified & Approved Domains" section of the site admin dashboard when one or more authoritative nameservers for

the affected domain were unreachable or unresponsive due to inefficient DNS queries.

- When migrating from an instance with S3 on AWS Gov Cloud, an incorrect URL was generated.
- Images embedded in Markdown tables did not display correctly.
- Deleted discussions could potentially prevent a repository from being exported using the export API or `ghe-migrator`.
- During an import, missing assignee models caused incomplete imports of issues, pull requests, and their dependent models.
- When the GitHub Enterprise Server application attempted to create an Elasticsearch index that already existed but lacked a routing configuration, the operation failed. This resulted in a state where the index appeared to exist, but the application could not write documents to it.
- Enterprise customers in very large organizations experienced performance issues with the GitHub API when making multiple API requests to retrieve Dependabot alerts for their enterprise.
- Instances using Azure for migration API storage without a proxy configured could not export migration archives because the system incorrectly attempted to route requests through a proxy.
- When administrators downloaded large Advanced Security committer CSV files, the operation would fail due to insufficient timeout settings. The timeout duration has been increased to ensure successful downloads.
- The "Grouped security updates" button was not being displayed in the Dependabot settings at the organization and repository levels.
- Actions workflows were not able to access up to 1,000 organization variables when the total size of all variables was under 10 MB.
- Fetches from repository caches returned a "Repository not found" error when the cache is out of sync.
- Secret scanning alerts would sometimes incorrectly identify the location of a secret in a file after a custom pattern was edited.

3.14.12: Changes

- Support tools now redact proxy credentials from their outputs in the admin terminal during connectivity checks.

- Live updates to the GitHub site were sometimes blocked by per-IP address rate limits, especially in environments where users accessed a GitHub Enterprise Server instance through a proxy.
- Merging a pull request using the "Rebase and merge" option is now limited to 100 commits. If you have a pull request with more than 100 commits, you can create a merge commit, or squash and merge, or split the commits into multiple pull requests.

3.14.12: Closing down

- Microsoft Exchange Online is retiring SMTP basic authentication during March-April 2026. If your GitHub Enterprise Server instance uses this method to send email, delivery may fail after the retirement date. Microsoft recommends switching to a supported alternative. As another option, you may consider using an SMTP OAuth proxy such as email-oauth2-proxy, though this is not officially supported. For details and configuration guidance, see the Microsoft announcement and the proxy's documentation. [Updated: 2025-09-03]

3.14.12: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.

- Running `ghe-cluster-config-apply` as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. The reindexing can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.

3.14.12: Errata

- The Known issues section previously indicated that `repository cache replicas return "Repository not found" when changes have been pushed to the primary instance that have not yet synchronized to the cache replica` is still an issue. The issue is resolved and is documented in the Bug fixes section. [Updated: 2025-06-19]

Enterprise Server 3.14.11

Download GitHub Enterprise Server 3.14.11

April 17, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.11: Security fixes

- **MEDIUM:** An attacker could view private repository names, which the signed-in user is not authorized to see, in the GitHub Advanced Security Overview. This was due to a missing authorization check and occurred when filtering with *only* `archived:`. GitHub has requested CVE ID CVE-2025-3124 for this vulnerability.

3.14.11: Bug fixes

- When restarting babeld, most commonly as part of upgrades between 3.14.x point releases, the old and new babeld processes could have a port conflict resulting in the babeld service stopping unexpectedly minutes or hours later.
- Pruning unreachable Git objects on a single replica could cause increased CPU load due to many Git checksum recalculations.
- In the commit author filter dropdown on the commit history page for a repository, users could not search for a specific author (such as `foo`) if their search query had already returned a similar username (such as `foobar`).
- Various repository content API endpoints were unable to parse revisions containing invalid UTF-8 byte sequences, triggering `500 Internal Server Error` responses.
- The "Get allowed actions and reusable workflows" APIs for enterprises, organizations, and repositories did not include the `verified_allowed` response field.

3.14.11: Changes

- Upgrading using a hot patch package will fail if the Elasticsearch status is not green. To help prevent post-upgrade problems when the Elasticsearch status is red, usually in a high-availability configuration, a check has been added.

- Merging a pull request using the "Rebase and merge" option is now limited to 100 commits. If you have a pull request with more than 100 commits, you need to either create a merge commit, or squash and merge, or split the commits up into multiple pull requests.
- The `spokesctl info` and `spokesctl repos` commands now also show wikis that are part of a network.

3.14.11: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens

via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.

- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- Services may respond with a `503` status due to an out of date `haproxy` configuration. This can usually be resolved with a `ghe-config-apply` run.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Repository Cache Replicas return `Repository not found` when changes have been pushed to the Primary instance that have not yet synchronized to the Cache Replica. This issue can also occur in all previous patches of this release.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.

Enterprise Server 3.14.10

Download GitHub Enterprise Server 3.14.10

March 25, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.10: Security fixes

- Packages have been updated to the latest security versions.

3.14.10: Bug fixes

- The `ghe-upgrade` command returned a zero exit code despite encountering errors.
- When performing an upgrade with an upgrade package, the process did not terminate when an invalid target partition was provided with the `-t` flag.
- Users could not use the `/manage/v1/config/apply` API endpoint to trigger the first configuration run on an instance.
- For instances in a high availability configuration, Elasticsearch indices were deleted on failover and when `ghe-repl-teardown REPLICA_HOSTNAME` was run from the primary instance. All indices are recoverable except audit log indices, whose source of truth is Elasticsearch itself.
- Restoring from a backup did not always apply the latest data from GitHub Actions. All GitHub Actions data is now restored with a backup.
- In Azure environments, running `ghe-single-config-apply` or `ghe-repl-setup` resulted in "Permission denied" errors during the pre-flight check.
- On instances with a GitHub Advanced Security license, some secret scanning alerts were opened incorrectly despite the relevant folders or files being excluded from secret scanning.
- For appliances in a high availability configuration, Elasticsearch indices were deleted either on failover, or when running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance.

3.14.10: Changes

- Elasticsearch shards are excluded from the replica node when stopping replication via `ghe-repl-stop`. To prevent Elasticsearch from being stopped before all shards have been removed, Elasticsearch is polled until the shard count on the replica node is zero instead of waiting for a maximum timeout of 30 seconds.
- Update the bundled `actions/setup-dotnet` with the latest versions from https://github.com/actions/setup-dotnet.

3.14.10: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.

- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.

Enterprise Server 3.14.9

Download GitHub Enterprise Server 3.14.9

March 04, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.9: Features

- Running GitHub Enterprise Server on the VMware ESXi 8.0 hypervisor is supported. If your installation is on VMware ESXi 7.x or earlier versions, you can now use the ESXi 8.0 hypervisor. [Updated: 2025-04-03]

3.14.9: Security fixes

- Permissions and ownership of `/etc/ssh/sshd_config` are now enforced so that the `root` identity is the only one able to read or write to the file.
- Packages have been updated to the latest security versions.

3.14.9: Bug fixes

- Some instances with self-signed certificates encountered duplicated IP and DNS entries in their certificate.

- During an upgrade, encrypted record diagnostics would incorrectly flag 2FA records without associated users as undecryptable, causing misleading or unactionable error messages. In addition, in a high-availability or cluster configuration, encrypted record diagnostics were run unnecessarily on nodes other than the MySQL primary, and the resulting prompt from these diagnostics did not honor the `-y` flag.
- An issue with the webhook delivery system could cause missing commits on pull requests and stop GitHub Actions workflows from running reliably on certain triggers. A database replication delay in the webhook delivery system has been removed.
- When a pre-receive hook blocked users from making a commit in the UI, the error message did not display any `echo` messages specified in the pre-receive hook script.
- When users requested large amounts of data from certain API endpoints, such as List organization repositories, they sometimes received a `500` error.
- Domain entries could fail to load in the "Verified & Approves Domains" section of the site admin dashboard if one or more authoritative nameservers for the affected domain was unreachable or unresponsive.
- Team avatars and descriptions did not always appear on the team's page.
- Some packages failed to install when a hotpatch was applied to instances hosted on Google Cloud Platform.

3.14.9: Changes

- The `ghe-check-disk-usage` command has been updated to provide more valuable insights into troubleshooting disk space issues on the root and data disks.
- A graph for visualizing the status of repository maintenance has been added to the management console.

3.14.9: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the

administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover

  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

    All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

    [Updated: 2025-03-19]

- After a restore, existing outside collaborators are unable to be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.

3.14.9: Errata

- The release notes previously did not mention VMware ESXi 8.0 support. [Updated: 2025-04-02]

Enterprise Server 3.14.8

Download GitHub Enterprise Server 3.14.8

February 18, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

> **Warning**: For instances installed on Google Cloud Platform (GCP), hotpatches to GitHub Enterprise Server version `3.14.8` will result in errors being reported in the upgrade log. We recommend hotpatching to a newer 3.14 version instead. [Updated: 2025-03-11]

3.14.8: Security fixes

- **HIGH**: An attacker could access environment variables in the debug artifacts uploaded by the CodeQL action after a failed code scanning workflow run. This includes any secrets that were

exposed to the workflow as environment variables. The attacker requires read access to the repository to access the debug artifact. Users who do not have debug logging enabled are unaffected. The impact to GitHub Enterprise Server users is limited to internal actors. To mitigate this issue, GitHub no longer logs the complete environment by default. GitHub has requested CVE-2025-24362 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- Packages have been updated to the latest security versions.

3.14.8: Bug fixes

- In some cluster configurations, it was not possible to enable GitHub Advanced Security in bulk.
- In certain cases, on an instance in a cluster configuration, secret scanning would fail to run due to misconfiguration of a Kafka service.
- In an instance in a high-availability or cluster configuration, administrators who updated the instance's license did not see the change reflected on the "Licenses" page in the UI.
- Audit log indices from 2018 could occasionally fail to be created when migrating to Elasticsearch 8.
- In some cases, a file in the code view would appear as JSON instead of HTML.
- Attachment records were not created when JWT tokens were included in user asset URLs on issues.
- When an administrator suspended a user from the site admin dashboard, the form required them to complete Digital Services Act (DSA) fields that are not relevant on GitHub Enterprise Server.
- Enterprise owners could not modify the "Outside collaborators" policy. Instead a `404 Not Found` response was returned.
- In cluster environments, API rate limits were calculated using the cluster node IP address instead of the client IP address. This could lead to incorrect rate limiting and the wrong IP address being recorded in audit log entries.
- The relative date for commits was sometimes incorrectly displayed in the web UI.
- Users were unable to open issues where the events timeline contained references to projects that were not moved over during a migration. Instead, the `500` error page was displayed.

- Users who had authenticated to multiple accounts, then logged out of one account, were unable to switch to a different account on the platform.
- Certain search terms for repositories and wikis did not return all valid results.
- In some cluster configurations, secret scanning failed to run normally due to connection failures.
- Images were not migrated properly when using GitHub Importer to import repositories from GitHub Enterprise Server.

3.14.8: Changes

- Log files on the appliance root disk are compressed immediately upon rotation daily instead of after a 24 hour delay. You can revert to the previous `delaycompress` behavior by signing in as an SSH admin user, setting `ghe-config logrotate.delaycompress true` and then running `ghe-config-apply`.
- The CodeQL Action has been updated to v3.28.6 to enable uploading artifacts in debug mode without logging the complete environment when running CodeQL CLI v2.20.3+.
- The `ghe-live-migrations --init-target` command fails with a descriptive error message if the specified upgrade path is not supported.

3.14.8: Known issues

- Instances installed on Google Cloud Platform (GCP) could experience errors when the latest hotpatch was applied. We recommend waiting for the next patch release to hotpatch. [Updated: 2025-03-11]
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.

- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

[Updated: 2025-03-12]

3.14.8: Errata

- The warning and known issues section have been updated to accurately reflect that instances installed on GCP will face issues while hotpatching to 3.14.8. Previously, the warning and known issue indicated that customers would face issues either while upgrading or hotpatching to version 3.14.8. [Updated: 2025-03-11]
- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.1, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.7

Download GitHub Enterprise Server 3.14.7

January 21, 2025

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.7: Security fixes

- **HIGH:** An attacker could forge a SAML response to provision and/or gain access to an account with administrator privileges for GitHub Enterprise Server instances that use SAML single sign-on authentication. Instances not utilizing SAML single sign-on or where the attacker is not already an existing user are not impacted. Exploitation of this vulnerability would allow for signature spoofing by improper validation. GitHub has requested CVE ID CVE-2025-23369 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

3.14.7: Bug fixes

- Restore failed silently on incremental MySQL backups.
- On an instance with GitHub Actions enabled, a configuration run could hang if the blob storage was inaccessible.
- Site administrators using `ghe-config-apply` saw `rm cannot remove DIRECTORY` errors. Old log directories are now removed without reporting errors.
- After an initial reboot, the appliance sometimes altered the ownership permissions of `gitmon` directories. As a result, the Management Console could hang at the "Starting" phase.
- The view for a repository's "top contributors" failed to render when when it received invalid parameters.
- Repository archive exports failed when the archive was more than 5 GiB.
- When users bypassed push protections for a file upload but did not re-add the file after the bypass was created, an incorrect error message displayed.
- The SAML SSO and SCIM identity of the user (actor) who performed the action, `external_identity_nameid`, was omitted from the metadata for audit log entries.
- If you unarchived a repository with secret scanning enabled and then enabled GitHub Advanced Security, the feature settings were incorrectly reported by security overview. Secret scanning was shown as disabled.
- `ghe-migrator` imports could fail due to attachments with invalid model types.

3.14.7: Changes

- To avoid service disruption, the bundled action `actions/setup-dotnet` uses new .NET CDN URLs. See https://github.com/dotnet/core/issues/9671.
- To avoid unnecessary error messages when users attempt to create a ruleset in evaluate mode in a repository that is user owned, we removed the evaluate mode option on the ruleset.

3.14.7: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.

- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:

  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.7: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.7, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.6

Download GitHub Enterprise Server 3.14.6

December 17, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.6: Security fixes

- Packages have been updated to the latest security versions.

3.14.6: Bug fixes

- On an instance in a cluster configuration, `ghe-repl-promote` failed if the primary node was unavailable.
- In a high availability configuration, with GitHub Actions, replication would fail on nodes where MSSQL was not configured to run.
- The `--no-async` flag was not implemented for the `ghe-cluster-support-bundle` command, leading to a potentially increased load.
- Pre-receive hook environments with shared memory enabled could not access shared memory at runtime.
- For instances hosted on Azure, if a pre-upgrade check failed due to insufficient user disk size, the Management Console displayed an internal server error.
- The Enterprise Overview page incorrectly displayed a Beta label, even though it is generally available.
- After a user made changes to the isolated subdomain setting, some user assets did not display properly.
- On an instance with secret scanning enabled, when selecting repositories for a dry run of an enterprise-level custom pattern, searches for full repository names (`ORGANIZATION/REPOSITORY`) did not return results.
- When adding bypass permissions to a ruleset, the dropdown menu failed to load if one of the suggested actors was an invalid integration.
- When creating a pre-receive hook environment, attempts to include an image URL over 255 characters failed with a database error. The maximum length is still 255 characters, but the URL length is now validated before the process starts.
- On an instance with GitHub Actions disabled, status check icons on a repositorys commit list failed to render.
- Site administrators were unable to use the "Disable repository access" functionality on the site admin dashboard.
- Attempting to access the code security settings page for a non-existent enterprise returned a 500 error instead of a 404 error.
- Performing a browser back navigation to a pull request now displays up-to-date status checks.
- Jekyll-build tooling for GitHub pages could fail when using the `jekyll-relative-links` plugin, see Failure details.

- The removal rate of issues from Git repositories was slower than necessary.

3.14.6: Changes

- Log output for git maintenance now includes the time taken to complete the maintenance process.
- When exporting repositories to blob storage using the migrations REST API endpoint to start an organization migration, the maximum compressed archive size is limited to 90 GB. This is an increase from 30 GB.
- Removes the minimum date for the new commit filter bar.
- When exporting repositories using the migrations REST API, prior to blob storage upload the tarball is staged in the root volume. For more disk capacity, the tarball will now be staged in the data volume.

3.14.6: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.

- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.6: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.6, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.5

Download GitHub Enterprise Server 3.14.5

December 03, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.5: Security fixes

- **LOW**: Instance administrators could see tokens used to authenticate against gitauth in plaintext in `/var/log/github-audit.log`.
- Packages have been updated to the latest security versions.

3.14.5: Bug fixes

- Embedded images in wiki pages were broken.

3.14.5: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- Attempting to stop replications after stopping GitHub Actions on a GitHub Enterprise Server instance would fail, reporting that MSSQL was not responding. This can be avoided by starting MSSQL prior to stopping replication `/usr/local/share/enterprise/ghe-nomad-jobs queue /etc/nomad-jobs/mssql/mssql.hcl`

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:

  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.5: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.5, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.4

Download GitHub Enterprise Server 3.14.4

November 12, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.4: Bug fixes

- Customers performing a feature version upgrade to 3.13.6 or 3.14.3 may experience issues with database migrations due to data issues during database conversions.

3.14.4: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.

- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.

- Attempting to stop replications after stopping GitHub Actions on a GHES instance would fail, reporting that MSSQL was not responding. This can be avoided by starting MSSQL prior to stopping replication `/usr/local/share/enterprise/ghe-nomad-jobs queue /etc/nomad-jobs/mssql/mssql.hcl`.

- When operating in a high availability configuration, running `ghe-repl-promote` on a replica node will fail if the original primary cannot be reached by the replica node. This is because the `ghe-repl-promote` script attempts to decommission all Elasticsearch nodes other than the promoted node, however these requests are made to the original primary node which is no longer reachable. The error message written to the terminal will be similar to:

  ```
  Maintenance mode has been enabled for active replica <REPLICA_HOSTNAME>
  {"message": "No server is currently available to service your request. Sorry
  about that. Please try resubmitting your request and contact your local GitHub
  Enterprise site administrator if the problem persists."}
  jq: error (at :3): Cannot index string with string "node"
  ```

  If this occurs, workaround this issue by running the following command — this changes the `ghe-repl-promote` script in place:

  ```
  sudo sed -i.bak -e '/for node_hostname in/i if ! $forced; then' -e '/^  done/a
  fi' /usr/local/bin/ghe-repl-promote
  ```

  Then re-run the updated `ghe-repl-promote` script.

  [Updated: 2024-11-29]

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:

  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.4: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.4, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.3

Download GitHub Enterprise Server 3.14.3

November 07, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.3: Security fixes

- Elasticsearch packages have been updated to the latest security versions.
- Packages have been updated to the latest security version.
- **HIGH**: An attacker could bypass SAML single sign-on (SSO) authentication with the optional encrypted assertions feature, allowing unauthorized provisioning of users and access to the instance, by exploiting an improper verification of cryptographic signatures vulnerability in GitHub Enterprise Server. This is a follow up fix for CVE-2024-9487 to further harden the encrypted assertions feature against this type of attack. Please note that encrypted assertions are not enabled by default. Instances not utilizing SAML SSO, or utilizing SAML SSO authentication without encrypted assertions, are not impacted. Additionally, an attacker would require direct network access as well as a signed SAML response or metadata document to exploit this vulnerability.
- **HIGH**: An attacker with Enterprise Administrator access to the GitHub Enterprise Server instance could escalate privileges to SSH root access. This is achieved by exploiting the pre-receive hook environment to bypass symlink checks in the `ghe-firejail` path and execute

malicious scripts. GitHub has requested CVE ID CVE-2024-10007 for this vulnerability, which was reported via the GitHub Bug Bounty program. [Updated: 2024-11-07]

- **HIGH**: An attacker could leak sensitive data from the DOM by injecting malicious input through the `identity` parameter in `querySelector` handling. This allows the attacker to dynamically embed a hidden iframe on the page and exfiltrate data from DOM attributes. To execute the attack, the victim must be logged into GitHub and interact with the attacker controlled malicious webpage containing the hidden iframe. GitHub has requested CVE ID CVE-2024-10001 for this vulnerability, which was reported via the GitHub Bug Bounty program. [Updated: 2025-01-27]

3.14.3: Bug fixes

- When saving settings in the Management Console, the configuration run would stop if the `enterprise-manage` process was restarted.
- On an instance with GitHub Actions enabled, some maintenance tasks could fail due to incomplete upgrade steps during previous upgrades to new releases of GitHub Enterprise Server.
- A repeated error message concerning connectivity to port 6002 was emitted to the system logs when GitHub Actions was enabled.
- The initial setup certificate generation in AWS took longer than expected due to fallback to private IPs. The time for this fallback has been reduced.
- The `ghe-support-bundle` generation would fail when the `aqueduct-lite` service is down.
- If the primary instance was unreachable, running `ghe-repl-stop --force` on a replica would fail during the config apply run.
- Administrators in the SCIM private beta (versions < 3.14) that decided to upgrade their private beta appliance see an incorrectly checked box in the "SCIM Configuration" section of the Enterprise settings authentication security page in 3.14.
- Certain URLs may have caused a 500 error on instances that use the mandatory message feature logging.
- When restoring from a backup, repositories that had been deleted in the last 90 days were not completely restored.
- For instances that use secret scanning, custom messages for push protection set by the enterprise did not display to users.
- Restoring Git repositories using `backup-utils` occasionally failed.

- Enterprise installations experienced unpredictable repository search results due to the default 4,000 repository limit. A relaxed repository filter mode, which includes all single-tenant organization repositories and bypasses the limit, has been introduced. Administrators can enable this mode using `ghe-config app.github.enterprise-repo-search-filter-enabled true && ghe-config-apply`.
- Running `config-apply` became stuck under certain circumstances due to a misconfiguration with Packages and Elasticsearch.
- Audit log events for secret scanning alerts incorrectly displayed a blank secret type when generated for a custom pattern.
- Some customers upgrading to 3.14 experienced issues with undecryptable records during the upgrade. This issue has now been resolved. A diagnostic script will run to assess impact, if no records are affected the message "SUCCESS: Encrypted records OK." will print to the console and can be ignored. If the error message "WARN: Error reading encrypted records!" is output, we recommend you read Undecryptable records. [Updated: 2024-01-22]

3.14.3: Changes

- When connecting to an appliance via SSH, a notification about upcoming root disk changes displays.

3.14.3: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. See Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.

- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a `config apply` as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- Customers doing feature version upgrade to 3.14.3 may experience issues with database migrations due to data issues during database conversions. [Added: 2024-11-08]
- When operating in a high availability configuration, running `ghe-repl-promote` on a replica node will fail if the original primary cannot be reached by the replica node. This is because the `ghe-repl-promote` script attempts to decommission all Elasticsearch nodes other than the promoted node, however these requests are made to the original primary node which is no longer reachable. The error message written to the terminal will be similar to:

```
Maintenance mode has been enabled for active replica <REPLICA_HOSTNAME>
{"message": "No server is currently available to service your request. Sorry
about that. Please try resubmitting your request and contact your local GitHub
Enterprise site administrator if the problem persists."}
jq: error (at :3): Cannot index string with string "node"
```

If this occurs, workaround this issue by running the following command — this changes the `ghe-repl-promote` script in place:

```
sudo sed -i.bak -e '/for node_hostname in/i if ! $forced; then' -e '/^  done/a
fi' /usr/local/bin/ghe-repl-promote
```

Then re-run the updated `ghe-repl-promote` script.

[Updated: 2024-11-29]

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.3: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.3, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.2

Download GitHub Enterprise Server 3.14.2

October 10, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.2: Security fixes

- A sensitive data exposure in HTML forms was possible in the management console. To mitigate this issue, the "Copy Storage Setting from Actions" functionality was removed from the management console.
- **MEDIUM**: Malicious URLs for SVG assets provided information about a victim user who clicked the URL, allowing an attacker to retrieve metadata belonging to the user and use it to generate a convincing phishing page. This required the attacker to upload malicious SVGs and phish a victim user to click the URL for the uploaded asset. GitHub has requested CVE ID CVE-2024-9539. This vulnerability was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker could bypass SAML single sign-on (SSO) authentication with the optional encrypted assertions feature, allowing unauthorized provisioning of users and access to the instance, by exploiting an improper verification of cryptographic signatures vulnerability in GitHub Enterprise Server. This was a regression introduced as part of follow-up remediation from CVE-2024-4985, which resulted in a new variant of the vulnerability. Please note that encrypted assertions are not enabled by default. Instances not utilizing SAML SSO, or utilizing SAML SSO authentication without encrypted assertions, are not impacted. Additionally, an attacker would require direct network access as well as a signed SAML response or metadata document. GitHub has requested CVE ID CVE-2024-9487. This vulnerability was reported via the GitHub Bug Bounty program.

3.14.2: Bug fixes

- A missing configuration value would cause Dependabot to be unable to create group update pull requests.
- HAProxy reloading was failure prone, which could lead to failed Git operations. This reloading process has been replaced with a more resilient Systemd process.
- This error message `mbind: Operation not permitted` was repeatedly showing in the `/var/log/mysql/mysql.err` MySQL logs.
- The backup of audit logs could take longer after upgrading to Elasticsearch 8.
- An unhandled nil value when configuring Actions storage with AWS S3 via OIDC configuration in the terminal could cause an error.

- Users were unable to sign out from gist pages.
- On an instance with secret scanning enabled, the custom pattern page would not load because dry run results were tied to a deleted repository.
- Suspended users were not always correctly routed to the correct "suspended" page.
- The "List teams" API endpoint returned duplicate results when paginating.
- When managing the organization permissions required for fine-grained personal access tokens, for custom properties or projects, the `Admin` access level could not be selected.
- A model with no URL could cause a `ghe-migrator` import to fail.
- The `ghe-spokesctl status` command showed repaired repositories as broken if their network ID changed during the repair (for example, when the repository was detached from it's original network).
- Missing URLs on import could lead to migration failures without logging or explanation.
- On the security overview dashboard, data initialization could fail when creating new organizations or changing GitHub Advanced Security licensing.
- Restore could fail when restoring MySQL using backup-utils.
- The help documentation for the Actions Workflow editor was not loading correctly. [Updated: 2025-02-18]

3.14.2: Changes

- `ghe-remove-node` will display the log file location when running in quiet mode.
- Pre-receive hook environments can use the `clone3()` system call.
- The creation, deletion, or change in visibility of a gist has been added to the audit log.

3.14.2: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone

with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- The admin stats REST API endpoints may time out on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- Images embedded in wiki pages may stop rendering shortly after being published. [Updated: 2024-10-16]

- When operating in a high availability configuration, running `ghe-repl-promote` on a replica node will fail if the original primary cannot be reached by the replica node. This is because the `ghe-repl-promote` script attempts to decommission all Elasticsearch nodes other than the promoted node, however these requests are made to the original primary node which is no longer reachable. The error message written to the terminal will be similar to:

  ```
  Maintenance mode has been enabled for active replica <REPLICA_HOSTNAME>
  {"message": "No server is currently available to service your request. Sorry
  about that. Please try resubmitting your request and contact your local GitHub
  Enterprise site administrator if the problem persists."}
  jq: error (at :3): Cannot index string with string "node"
  ```

  If this occurs, workaround this issue by running the following command — this changes the `ghe-repl-promote` script in place:

  ```
  sudo sed -i.bak -e '/for node_hostname in/i if ! $forced; then' -e '/^  done/a
  fi' /usr/local/bin/ghe-repl-promote
  ```

  Then re-run the updated `ghe-repl-promote` script.

  [Updated: 2024-11-29]

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:

  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.2: Deprecations

- The option to "copy Storage settings from Actions" in the Management Console ("GitHub Packages" > "Packages Storage Settings") has been removed. [Updated: 2024-11-20]

3.14.2: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.2, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.1

Download GitHub Enterprise Server 3.14.1

September 23, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.14.1: Security fixes

- **MEDIUM:** An attacker could steal sensitive information by exploiting a Cross-Site Scripting vulnerability in the repository transfer feature. This exploitation would require social engineering. GitHub has requested CVE ID CVE-2024-8770 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH:** A GitHub App installed in organizations could upgrade some permissions from read to write access without approval from an organization administrator. An attacker would require an account with administrator access to install a malicious GitHub App. GitHub has requested CVE ID CVE-2024-8810 for this vulnerability, which was reported via the GitHub Bug Bounty Program. [Updated: 2024-11-07]

3.14.1: Bug fixes

- On an instance with GitHub Actions enabled, due to an insufficient wait time, MS SQL and MySQL replication could fail with the error message `Failed to start nomad service!`.
- `ghe-storage-find` was sometimes unable to identify a data disk.

- After upgrading the relevant GHES version, the `resolvconf` service failed to start due to a missing directory.
- Some pre-receive hooks using the `faccessat2` system call, such as those using Alpine Linux as the base, failed unexpectedly.
- When configuring a high availability replica and during the database seeding of a MySQL replica node, restarting the nomad service could time out. Consequently, when MySQL replication attempted to start an error was reported, and setting up replication failed.
- On an instance in a cluster configuration, the `ghe-cluster-status` command returned an error if a soft-deleted repository had a checksum mismatch.
- Fixes and improvements for the git core module.
- Some repositories could miss spokes information after restoring in a clustering topology due to unrescued exceptions.
- In organizations with a large number of repositories, when an administrator used repository properties to target repositories in an organization ruleset, the ruleset index page timed out.
- After a user created a Projects Insights chart with time as the X-axis, the chart became hidden and inaccessible.
- Fixes a known issue where some links to GitHub Docs from GitHub Enterprise Server may lead to a “Page not found.” Previously, the links incorrectly added `enterprise-cloud@latest` to the URL.
- A bug introduced in 3.12 which prevented the search input in the global navigation from displaying a dropdown of search suggestions has been fixed. The search input functionality prior to 3.12 has been restored, and users are once again able to see and submit suggested search queries, including scope suggestions.
- Custom links to other repositories displayed incorrect breadcrumbs.
- The Secret Scanning Push Protection custom resource link set at the Enterprise level was not being displayed to users being blocked when pushing secrets to a repository using git through the command line interface.
- Following an upgrade, Elasticsearch search migrations are sometimes incorrectly reported as failing in the audit log, even though the migrations completed successfully. [Updated: 2024-09-27]

3.14.1: Changes

- For instances deployed on Amazon Web Services (AWS), site administrators can configure regional AWS STS endpoints for OIDC from the Management Console.
- Site administrators can now configure the instance with NUMA optimizations.

3.14.1: Known issues

- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as `127.0.0.1`.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance onto a 3.13 appliance, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.

- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- Services may respond with a `503` status due to an out of date `haproxy` configuration. This can usually be resolved with a `ghe-config-apply` run.
- Images embedded in wiki pages may stop rendering shortly after being published. [Updated: 2024-10-16]
- When operating in a high availability configuration, running `ghe-repl-promote` on a replica node will fail if the original primary cannot be reached by the replica node. This is because the `ghe-repl-promote` script attempts to decommission all Elasticsearch nodes other than the promoted node, however these requests are made to the original primary node which is no longer reachable. The error message written to the terminal will be similar to:

  ```
  Maintenance mode has been enabled for active replica <REPLICA_HOSTNAME>
  {"message": "No server is currently available to service your request. Sorry
  about that. Please try resubmitting your request and contact your local GitHub
  Enterprise site administrator if the problem persists."}
  jq: error (at :3): Cannot index string with string "node"
  ```

  If this occurs, workaround this issue by running the following command — this changes the `ghe-repl-promote` script in place:

  ```
  sudo sed -i.bak -e '/for node_hostname in/i if ! $forced; then' -e '/^  done/a
  fi' /usr/local/bin/ghe-repl-promote
  ```

  Then re-run the updated `ghe-repl-promote` script.

  [Updated: 2024-11-29]

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover

- When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

[Updated: 2025-03-12]

3.14.1: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.1, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

Enterprise Server 3.14.0

Download GitHub Enterprise Server 3.14.0

August 27, 2024

📣 This is not the latest patch release of this release series, and this is not the latest release of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

For upgrade instructions, see Upgrading GitHub Enterprise Server.

3.14.0: Features

- **Instance administration**
  - On an instance with multiple replica nodes, to start or stop replication for all nodes in a single configuration run, administrators can use the `ghe-repl-start-all` and `ghe-repl-stop-all` commands.

- **Instance services**
  - Administrators can scale the appliance using generation 2 virtual machines, with support for booting in UEFI mode. This requires deploying a new instance and restoring data onto it. See Using generation 2 virtual machines.
  - Nomad has been upgraded to 1.5.17 and Consul has been upgraded to 1.17.4. These services are used in GitHub Enterprise Server to orchestrate containers and configuration.

- **Identity and access management**
  - Automated user provisioning via the System for Cross-domain Identity Management (SCIM) standard is available in public beta. Instances that use SAML authentication can enable SCIM to provision user accounts and manage their lifecycle from an identity provider (IdP). You can configure SCIM using an application for supported IdPs, or using the REST API endpoints for SCIM. See About user provisioning with SCIM on GitHub Enterprise Server.
    - If your instance already uses SAML, you will need to configure a new IdP application that supports automated provisioning via SCIM.
    - Existing private beta customers should also reconfigure their implementation with an updated application.
    - During the public beta, we recommend testing SCIM support for your identity system in a non-production instance before adding SCIM to your current setup.
  - Organization owners can create and assign custom organization roles, delegating administrative duties to trusted teams and users. See Managing custom organization roles.
  - Users can use the account switcher to switch between multiple accounts. See Switching between accounts.
  - On an instance that uses built-in authentication, users can use passkeys to sign in securely to GitHub, without needing to input their password. See Authenticating with a passkey.
  - Enterprises that use an SSH certificate authority can allow SSH certificates to be used to access user-owned repositories. See Enforcing policies for security settings in your enterprise.

- **Audit logs**
  - Every 24 hours, a health check runs for each audit log stream. If a stream is set up incorrectly, an email will be sent to the enterprise owners as notification that their audit log

stream is not properly configured.

- **Secret scanning**
  - Users can specify which teams or roles have the ability to bypass push protection. This feature is in public beta and subject to change. See About push protection.
  - Secret scanning detects secrets leaked in discussions and in pull request titles, bodies, and comments. This feature is in public beta and subject to change. See About secret scanning.
  - Secret scanning blocks contributors from uploading files with detected secrets if push protection is enabled for a repository. This feature is in public beta and subject to change.
  - Audit log events are created when secret scanning non-provider patterns are enabled or disabled at the repository, organization, or enterprise level.

- **Code scanning**
  - Users can create a dedicated code scanning rule to block pull request merges, instead of relying on status checks. This feature is in public beta and subject to change. See Set code scanning merge protection.
  - Users can use CodeQL threat model settings for C# to adapt CodeQL's code scanning analysis to detect the most relevant security vulnerabilities in their code. This feature is in public beta and subject to change. See Editing your configuration of default setup.
  - Organizations that use default setup for code scanning can use organization-level model packs to extend the coverage of multiple repositories. This feature is in public beta and subject to change. See Editing your configuration of default setup.
  - CodeQL can scan Java projects without a build. This feature is in public beta and subject to change.
  - This release comes installed with version **2.17.6** of the CodeQL CLI, used in the CodeQL action for code scanning. Significant updates since the default version installed on GitHub Enterprise Server 3.13 include:
    - Support for Java 22, Swift 5.10, TS 5.4, and C# 12
    - New queries for C/C++, Go, Java, and Ruby:
      - `cpp/type-confusion`: Detects casts to invalid types

    - `cpp/iterator-to-expired-container`: Detects the creation of iterators owned by temporary objects that are about to be destroyed
    - `go/uncontrolled-allocation-size`: Detects slice memory allocation with excessive size value
    - `java/unvalidated-url-forward`: Prevents information disclosure caused by unsafe URL construction
    - `rb/insecure-mass-assignment`: Detects instances of mass assignment operations accepting arbitrary parameters
    - `rb/csrf-protection-not-enabled`: Detects cases where Cross-Site Request Forgery protection is not enabled in Ruby on Rails controllers

- **Dependabot**
    - Users can consolidate Dependabot pull requests by enabling grouped security updates for related dependencies in a package ecosystem. See About Dependabot security updates.
    - Dependabot can access Cargo private registries to provide updates to Rust dependencies. See Guidance for the configuration of private registries for Dependabot.
    - Dependabot pauses scheduled jobs after 15 failures. This gives an earlier indication of potential issues while still ensuring that critical security updates continue to be applied without interruption.
    - Dependabot uses private registry configurations specified in the `dependabot.yml` file as expected, even if there is a configuration with `target-branch`. This ensures that security updates are applied correctly, regardless of your repository's configuration settings. See Configuring access to private registries for Dependabot.
    - In the `dependabot.yml` file, users can apply the same configuration to manifest files from multiple directories using the `directories` key. Direct strings, glob syntax, and wildcards (`*`) are all supported for targeting directories. See Dependabot options reference. [Updated: 2024-10-07]

- **Code security**
    - The security overview dashboard, with the ability to view secret scanning metrics and trending data for the enablement of security features, is available at the enterprise level. See Viewing security insights.
    - The security overview dashboard for organizations is now generally available.

  - On the security overview dashboard, users can view alert trends grouped by tool. The group-by option is designed to improve the ability to track and analyze the effectiveness of scanning tools, enabling more strategic decision-making. See Viewing security insights.
  - On the security overview dashboard, users can filter by security tool. This feature is in public beta and subject to change.
  - In the dependency graph, a software bill of materials (SBOM) generated for a package now includes the package URL for more packages. Previously, the package URL was not included if the manifest file referenced a package with a version range.

- **GitHub Actions**
  - For self-hosted GitHub Actions runners on this GitHub Enterprise Server release, the minimum required version of the GitHub Actions Runner application is 2.317.0. See the release notes for this version in the `actions/runner` repository. If your instance uses ephemeral self-hosted runners and you've disabled automatic updates, you must upgrade your runners to this version of the Runner application before upgrading your instance to this GitHub Enterprise Server release.
  - Deployment views across environments are now generally available. Users can pin environments and use additional filters to filter the views. See Viewing deployment history.

- **GitHub Pages**
  - Users can configure custom GitHub Actions workflows to build and deploy sites on GitHub Pages. See Configuring a publishing source for your GitHub Pages site.

- **Repositories**
  - Users can enhance security by adding deploy keys as a bypass type to rulesets. See Creating rulesets for a repository.
  - Users can select Dependabot in the bypass list of a ruleset. See Creating rulesets for a repository.

- **Projects**
  - Users can use the auto-close issue workflow to automatically close issues when a project item moves to a specific "completed" status. See Using the built-in automations.

- **Integrations and extensions**
  - When authenticating to a native GitHub App or OAuth app, users will be prompted to select which account they want to sign in to using an account picker. Developers of apps can append `?prompt=select_account` to their login flow to show users the account picker.
  - When using a JSON Web Token (JWT) to authenticate or request an installation token, developers of GitHub Apps can use the app's client ID for the JWT's `iss` claim. The application ID remains valid, but is considered deprecated.

3.14.0: Changes

- The API endpoint for setting and removing organization membership for a user (`PUT /orgs/{org}/memberships/{username}` and `DELETE /orgs/{org}/memberships/{username}`) requires `admin:org` permissions for classic tokens. Previously, the changes were allowed with the `read:org, repo` permissions. [Updated: 2025-07-16]

3.14.0: Known issues

- Complete SCIM payloads are written to the audit log, including SCIM attributes that are not required or supported per API docs. Customers using Okta with SCIM may notice that a placeholder password attribute is among the data passed to audit logs in its current configuration. This placeholder data is associated with Okta's password synchronization feature that is not expected or required by GitHub. See okta-scim for more information.
- Custom firewall rules are removed during the upgrade process.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.

- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- REST API endpoints for admin stats may time out on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shut down the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 appliance, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- The global search bar does not have suggestions enabled due to the redesigned navigation and pending new search experience.
- Upgrades include an error concerning `Error deregistering job` for `consul-template`. This message does not indicate any problems with your install and can be safely ignored.
- Some links to GitHub Docs from GitHub Enterprise Server may lead to a "Page not found," because an `enterprise-cloud@latest` portion is incorrectly added to the URL.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- In the header bar displayed to site administrators, some icons are not available.
- When restoring from a backup snapshot, a large number of `mapper_parsing_exception` errors may be displayed.
- On boot, the `resolvconf` service may fail to start because the `/run/resolvconf` directory does not exist when the service attempts to `touch` a file there, with the error:

```
/bin/touch: cannot touch '/run/resolvconf/postponed-update': No such file or
directory
```

If this occurs, workaround this issue with the following commands — this change will persist on reboots, but not upgrades:

```
sudo sed -i.bak \
'/\[Service\]/a ExecStartPre\=\/bin\/mkdir \-p \/run\/resolvconf' \
/etc/systemd/system/resolvconf.service.d/local.conf

sudo systemctl daemon-reload
sudo systemctl start resolvconf
```

- Services may respond with a 503 status due to an out of date haproxy configuration. This can usually be resolved with a `ghe-config-apply` run.
- When enabling automatic update checks for the first time in the Management Console, the status is not dynamically reflected until the "Updates" page is reloaded.
- Following an upgrade, Elasticsearch search migrations are sometimes incorrectly reported as failing in the audit log, even though the migrations completed successfully. [Updated: 2024-09-27]
- Images embedded in wiki pages may stop rendering shortly after being published. [Updated: 2024-10-16]
- When operating in a high availability configuration, running `ghe-repl-promote` on a replica node will fail if the original primary cannot be reached by the replica node. This is because the `ghe-repl-promote` script attempts to decommission all Elasticsearch nodes other than the promoted node, however these requests are made to the original primary node which is no longer reachable. The error message written to the terminal will be similar to:

  ```
  Maintenance mode has been enabled for active replica <REPLICA_HOSTNAME>
  {"message": "No server is currently available to service your request. Sorry
  about that. Please try resubmitting your request and contact your local GitHub
  Enterprise site administrator if the problem persists."}
  jq: error (at :3): Cannot index string with string "node"
  ```

  If this occurs, workaround this issue by running the following command — this changes the `ghe-repl-promote` script in place:

```
sudo sed -i.bak -e '/for node_hostname in/i if ! $forced; then' -e '/^  done/a
fi' /usr/local/bin/ghe-repl-promote
```

Then re-run the updated `ghe-repl-promote` script.

[Updated: 2024-11-29]

- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

  All indices are recoverable, except for Audit Log indices. Since Elasticsearch itself is the source of truth for these logs, they may only be recoverable from a backup. If you need assistance, visit GitHub Enterprise Support.

  [Updated: 2025-03-12]

3.14.0: Deprecations

- The Manage GHES API reached feature parity with the Management Console API in GHES 3.12. As a result, we will remove the Management Console API in GitHub Enterprise Server 3.15. For information about updating tooling that relies on the Management Console API, see REST API endpoints for Management Console.
- Team discussions have been removed from GitHub Enterprise Server. The sunset of this feature was announced in 2023. See the GitHub Blog post. [Updated: 2025-02-13]
- Node 16 support ended in September 2023. Actions that used Node 16 now default to Node 20. Running a workflow that uses Node 16 results in a warning on the workflow summary page. [Updated: 2025-04-02]

3.14.0: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.0 when log forwarding is enabled, some forwarded log entries may be duplicated. The fix for this problem was already included prior to the release of GitHub Enterprise Server 3.14.0. [Updated: 2024-09-16]

- These release notes did not include a note for support of the `directories` key in `dependabot.yml` files. [Updated: 2024-10-07]

- The "Changes" section indicated that "Pushes that update over 5,000 branches no longer trigger webhooks or GitHub Actions workflows." The change instead affects GitHub Enterprise Server version 3.15. [Updated: 2024-10-30]

- These release notes previously did not include a note for the deprecation of team discussions.

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.14.0, repositories originally imported using `ghe-migrator` will not correctly track Advanced Security contributions.

  The fix for this problem was already included in GitHub Enterprise Server 3.12. [Updated: 2025-04-11]

- The release notes previously did not include a note for the change in permissions required for managing user organization membership. [Updated: 2025-07-16]