> **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 3.15 release notes**

---

# Enterprise Server 3.15.21

Download GitHub Enterprise Server 3.15.21

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.

---

## 3.15.21: 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to private repositories by abusing scoped user-to-server (`ghu_`) tokens after their associated GitHub App installation was revoked or deleted.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.

- **LOW**: GitHub Enterprise Server included React versions 19.0, 19.1, and 19.2 in its package, which contain vulnerabilities in the React Server Components protocol (CVE-2025-55182, CVE-2025-66478). GitHub Enterprise Server does not use React Server Components and was not vulnerable to exploitation. React has been updated to version 19.2.3 to address findings from security scanning tools.

## 3.15.21: 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.
- On instances connected to GitHub Enterprise Cloud with data residency, the "GitHub.com actions" setting appeared in the GitHub Connect configuration despite this feature not being available for data residency deployments.
- The site admin bar displayed debugging information used by GitHub.
- Suspended users were listed in an organization's list of members.
- 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.

### 3.15.21: Changes

- Administrators can now set `mysql.innodb-online-alter-log-max-size` with `ghe-config` so the value persists when a configuration is applied or upgraded.

### 3.15.21: 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 an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.

- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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-`



- Unexpected elements may appear in the UI on the repo overview page for locked repositories.
- GitHub Enterprise Server releases shipped with mismatched Git versions between containers.

## Enterprise Server 3.15.20

Download GitHub Enterprise Server 3.15.20

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.

### 3.15.20: 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.

## 3.15.20: 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.
- On the dependency graph page, users saw a banner promoting automatic dependency submission despite the feature being unavailable on GitHub Enterprise Server. The banner also linked to documentation that was inaccessible.
- 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.

## 3.15.20: 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.
- On instances with a license for GitHub Advanced Security, code scanning-specific rate limits have been lifted and aligned with the default GitHub rate limits. Users can access higher limits

through an exemption mechanism.

### 3.15.20: Known issues

- During an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.
- When initializing a new cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Administrators setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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 3.15.19

Download GitHub Enterprise Server 3.15.19

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 3.15.19 has been unpublished due to mismatched Git versions between containers. Please use the most recent available patch release of 3.15. [Updated: 2026-03-13]

## 3.15.19: 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.

## 3.15.19: 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.

- On the dependency graph page, users saw a banner promoting automatic dependency submission despite the feature being unavailable on GitHub Enterprise Server. The banner also linked to documentation that was inaccessible.
- 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.

## 3.15.19: 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.
- On instances with a license for GitHub Advanced Security, code scanning-specific rate limits have been lifted and aligned with the default GitHub rate limits. Users can access higher limits through an exemption mechanism.

## 3.15.19: 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 an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Administrators setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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 3.15.18

Download GitHub Enterprise Server 3.15.18

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.

---

### 3.15.18: Features

- Administrators can configure advanced SMTP settings for improved email delivery performance and reliability. These settings map to Postfix configuration parameters as documented in the Postfix documentation. New options include:
  - IPv4-only relay: Route email to addresses at a specific email domain through an IPv4-only relay host. Setting `smtp.ipv4-only` to `true` configures Postfix to route all email to the domain specified in `smtp.relay-domain` through `smtp.relay-host` on port `smtp.relay-port` using IPv4 only.
  - Connection caching: Control connection reuse and caching (`smtp.connection-cache-time-limit`, `smtp.connection-reuse-count-limit`, `smtp.connection-cache-on-demand`).
  - Delivery concurrency: Tune parallel email delivery limits (`smtp.destination-concurrency-limit`, `smtp.initial-destination-concurrency`, `smtp.destination-concurrency-positive-feedback`).

  - Queue management: Configure retry timing and queue processing (`smtp.maximal-backoff-time`, `smtp.queue-run-delay`)
  - Connection limits: Set maximum inbound SMTP connections (`smtp.client-connection-count-limit`).

## 3.15.18: 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.

## 3.15.18: 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.
- Push rejections due to custom pre-receive hooks were not visible in the audit log.
- Users could only view webhook deliveries from the previous three days.

## 3.15.18: 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.

### 3.15.18: Known issues

- During an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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 3.15.17

Download GitHub Enterprise Server 3.15.17

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.

---

## 3.15.17: 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-2026-2304 for this vulnerability, which was reported via the GitHub Bug Bounty program.

## 3.15.17: 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.
- In the "Password and authentication policies" section of the Management Console, administrators could specify invalid values for the "Login attempt limit for all users" and "Lockout time for Management Console users" settings, because inputs were not correctly validated.
- The highlighted section on the sidebar of the Management Console settings page did not always accurately reflect the content currently scrolled into view.
- 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 could encounter inaccurate free disk space calculations when setting Elasticsearch watermarks, as incorrect methods were used for determining root and data disk sizes.
- 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.
- When administrators enabled GitHub Advanced Security features in bulk, enablement progress was not always tracked accurately. As a result, subsequent bulk scans for GitHub Secret

Protection could be triggered or grouped incorrectly.

### 3.15.17: 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.

### 3.15.17: Known issues

- During an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.
- When initializing a new cluster, nodes with the `consul-server` role should be added to the cluster before adding more nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Administrators setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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 3.15.16

Download GitHub Enterprise Server 3.15.16

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.

## 3.15.16: 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.

## 3.15.16: 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.

## 3.15.16: Known issues

- Custom firewall rules are removed during the upgrade process.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.

- 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 3.15.15

Download GitHub Enterprise Server 3.15.15

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.

---

### 3.15.15: 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.

## 3.15.15: 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 instances 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.
- Site administrators using the Management Console would see overly verbose error messages on the maintenance page. These error messages were not cleared when a new request was made, and no message was displayed when maintenance mode changes were saved successfully.
- An "Invite member" button intended only for GitHub.com was displayed on the enterprise "People" tab.
- Link previews did not appear in Slack conversations when messages were delivered through socket mode, affecting the visibility of linked GitHub content.
- 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.

## 3.15.15: 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]

### 3.15.15: Known issues

- Custom firewall rules are removed during the upgrade process.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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 3.15.14

Download GitHub Enterprise Server 3.15.14

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.

---

## 3.15.14: 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.

## 3.15.14: Bug fixes

- Users applying a new license file received an HTTP 500 error.
- Administrators running the `ghe-repl-start-all` command may have encountered replicas remaining in an enabled state after a failed operation, causing subsequent configuration updates to execute on unintended nodes. Replicas now revert to a disabled state if the command fails.
- Setting up MySQL replication on secondary replica nodes was inefficient and consumed unnecessary root disk space.
- When running the `system-requirements` check as part of the `ghe-cluster-config-check` command prior to the initialization of a new cluster, the check request would fail because it exceeded the overall request timeout.
- SVG files stored in Git Large File Storage (LFS) failed to render on the web interface.
- Announcements scheduled using the `expires_at` timestamp in ISO 8601 format were not parsing the specified time correctly, resulting in the time component always being ignored.
- On the "Scheduled workflows" page in the site admin dashboard, actors attributed to workflows appeared as "Not found".

- On instances where GitHub Actions workflows require approval to run on pull requests from forked repositories, workflows remained queued indefinitely after users clicked "Approve and run".

### 3.15.14: 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.

### 3.15.14: Known issues

- Custom firewall rules are removed during the upgrade process.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding more nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Unexpected elements may appear in the UI on the repository overview page for locked repositories.

# Enterprise Server 3.15.13

Download GitHub Enterprise Server 3.15.13

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.

---

## 3.15.13: Security fixes

- Packages have been updated to the latest security versions.

## 3.15.13: 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.
- 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.
- Administrators debugging Elasticsearch index repairs previously did not see a "starting" log entry before a repair began, making it harder to track repair initiation in logs.

## 3.15.13: Changes

- For administrators managing logs, log folders are more consistently accessible from the administrative account without the need to use `sudo`.
- Administrators can no longer run the `ghe-upgrade` command on a replica node if a configuration apply is running or has failed on the primary node. This change helps prevent upgrade conflicts and ensures more reliable high availability maintenance workflows.
- Administrators monitoring Elasticsearch index repair jobs benefit from improved log clarity. Log messages provide more detailed and actionable information, making it easier to troubleshoot and track the progress of index repair operations.

### 3.15.13: Known issues

- Custom firewall rules are removed during the upgrade process.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Unexpected elements may appear in the UI on the repo overview page for locked repositories.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.15.12

Download GitHub Enterprise Server 3.15.12

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.

---

> **Warning**: We are lifting the pause on upgrade to 3.15. You can now upgrade to version 3.15.12, but not to earlier releases of 3.15. This release includes optimizations that address performance issues reported in recent versions of GitHub Enterprise Server. As an additional step, it is recommended to check system capacity before upgrading. See check system capacity before upgrading.

### 3.15.12: 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.
- The maintenance page in the Management Console did not include cross-site request forgery (CSRF) protection.

### 3.15.12: Bug fixes

- For enterprises with a large number of organizations, some authorization queries were non-performant. This patch includes a set of fixes improving the performance of authorization checks that enforce PAT access policies for both fine-grained and classic Personal Access Tokens (PATs).
- On instances in a cluster configuration, builds of GitHub Pages sites timed out in GitHub Actions workflows.
- 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.
- 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.

- Site administrators observed that uploading a license failed to restart GitHub services after upgrading GitHub Enterprise Server due to file permission issues in `/var/log/license-upgrade`.
- After upgrading to 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]

## 3.15.12: 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.
- Configuration runs do not output transient Elasticsearch health check failures. This update reduces log verbosity to address confusion reported by users.
- For administrators monitoring search index repairs, logs for repair jobs now include batch-level details, such as the ranges of updated IDs. This improvement makes it easier to track and debug the status of index repairs.

## 3.15.12: 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 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES

3.15.14 or higher.

[Updated: 2025-11-24]

---

## Enterprise Server 3.15.11

Download GitHub Enterprise Server 3.15.11

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.11: Security fixes

- Packages have been updated to the latest security versions.

### 3.15.11: 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.
- Enterprise Managed Users (EMUs) who were restricted from creating user namespace repositories could still create repositories in organizations and transfer them to their user namespace.

- On instances with secret scanning enabled, repositories could display a persistent backfill banner due to pending scans associated with canceled job groups.
- Administrators and users could experience delays due to performance regressions affecting the background processing of notification jobs.

### 3.15.11: Changes

- For administrators performing a live upgrade, a new entry point has been added to the upgrade container to clean up database tables. This utility can be run manually via `ghe-live-migrations -cleanup`, and is also executed automatically via `ghe-config-apply` after a complete upgrade.
- During pre-upgrade operations of a live upgrade, tables are now renamed instead of being dropped immediately. The tables are then dropped at a later stage via `ghe-config-apply`.

### 3.15.11: 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- 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]

- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.15.10

Download GitHub Enterprise Server 3.15.10

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.10: 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.

### 3.15.10: 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.

### 3.15.10: Changes

- Site administrators can now set `innodb_buffer_pool_size` in megabytes for MySQL using `ghe-config mysql.innodb-buffer-pool-size VALUE`.
- Site administrators running migrations on GitHub Enterprise Server benefit from optimized performance for code scanning, as garbage collection-related `ts_analyses` migrations are combined into a single step. This reduces migration time and minimizes operational disruption during upgrades.

### 3.15.10: 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

# Enterprise Server 3.15.9

Download GitHub Enterprise Server 3.15.9

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.

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

## 3.15.9: Security fixes

- Packages have been updated to the latest security versions.

## 3.15.9: 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.
- The secret scanning metrics page displayed data for expired delegated bypass requests.
- When users added a team with a repository role to the `CODEOWNERS` file, an unknown error was displayed. Teams with repository roles are now correctly recognized as valid owners of files.

## 3.15.9: Changes

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

## 3.15.9: 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.15.8

Download GitHub Enterprise Server 3.15.8

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.8: 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.

### 3.15.8: Bug fixes

- The Management Console maintenance page would not load correctly if the underlying API call fails to load the connection services data.
- 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.
- On instances with a large number of code scanning users, running `ghe-config-apply` previously resulted in slow performance.
- 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.
- 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]

### 3.15.8: Changes

- To ensure critical integrations and automated systems have uninterrupted access, the `/repositories/:repository_id/collaborators` endpoints now honor the higher rate limits for exempt users set with `ghe-config app.github.rate-limiting-exempt-users "<USER>"`.
- 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.

### 3.15.8: 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.

### 3.15.8: 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES

3.15.14 or higher.

[Updated: 2025-11-24]

---

## Enterprise Server 3.15.7

Download GitHub Enterprise Server 3.15.7

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.7: 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.

### 3.15.7: 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 erroneous error `ERROR: Failed to get elastomer index build progress` being 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.
- 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.
- 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.
- Pull request pages did not update asynchronously to reflect new changes, sometimes causing users to see outdated information until a manual refresh or navigation occurred.
- On instances where vulnerability alerts were not configured, server usage metrics did not upload as expected.
- 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.

### 3.15.7: 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 access the 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.

### 3.15.7: 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]

### 3.15.7: 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 `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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding more nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Administrators setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

### 3.15.7: 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 3.15.6

Download GitHub Enterprise Server 3.15.6

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.6: 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.

### 3.15.6: Bug fixes

- 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.
- Pull requests notifications in Slack and Teams integrations did not strikethrough in the UI when approved.

### 3.15.6: 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.

### 3.15.6: 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 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

# Enterprise Server 3.15.5

Download GitHub Enterprise Server 3.15.5

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

## 3.15.5: Security fixes

- Packages have been updated to the latest security versions.

## 3.15.5: Bug fixes

- In Azure environments, running `ghe-single-config-apply` or `ghe-repl-setup` resulted in "Permission denied" errors during the pre-flight check.
- 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.
- 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.
- 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.

## 3.15.5: 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.

### 3.15.5: 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 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

## Enterprise Server 3.15.4

Download GitHub Enterprise Server 3.15.4

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.4: 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]

### 3.15.4: 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.

### 3.15.4: 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.

### 3.15.4: 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.

### 3.15.4: 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 steps for [Replacing the primary MySQL node]/admin/monitoring-managing-and-updating-your-instance/configuring-clustering/replacing-a-cluster-node#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.
- 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.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running ghe-cluster-repl-status if a new organization and repositories are created before using the ghe-cluster-repl-bootstrap command. To avoid this issue, complete the cluster HA setup with ghe-cluster-repl-bootstrap before creating new organizations and repositories.
- 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.

- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

### 3.15.4: Errata

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

---

## Enterprise Server 3.15.3

Download GitHub Enterprise Server 3.15.3

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**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

> **Warning**: For instances installed on Google Cloud Platform (GCP), hotpatches to GitHub Enterprise Server version `3.15.3` will result in errors being reported in the upgrade log. We recommend hotpatching to a newer 3.15 version instead. [Updated: 2025-03-11]

### 3.15.3: Security fixes

- **LOW**: An attacker with access to an organization administrator's user account could view repository metadata without an active SAML SSO session by searching for repositories within the organization and viewing the search results.
- **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.

### 3.15.3: Bug fixes

- After disabling the "TLS only" setting in the Management Console, the maintenance page failed to load.
- 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.
- Attachment records were not created when JWT tokens were included in user asset URLs on issues.
- In some cases, a file in the code view would appear as JSON instead of HTML.

- 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.
- The relative date for commits was sometimes incorrectly displayed in the web UI.
- 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.
- 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.
- 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.

### 3.15.3: Changes

- Log files on the appliance root disk are compressed immediately upon daily rotation 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 logrotate `maxsize` (the maximum size of the log file before rotation) automatically scales to 5% of the current root partition size, instead of the prior static value of 15G. This better protects the root disk from unexpected large log files filling up the volume. Administrators can run `ghe-config logrotate.maxsize` to change the configuration value to a static value. Full cluster environments are excluded from this change and retain the 15G static value, unless overridden.
- 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.

### 3.15.3: 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

## 3.15.3: Errata

- The warning and known issues section have been updated to accurately reflect that instances installed on GCP will face issues while hotpatching to 3.15.3. Previously, the warning and known issue indicated that customers would face issues either while upgrading or hotpatching to version 3.15.3. [Updated: 2025-03-11]

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.15.3, 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 3.15.2

Download GitHub Enterprise Server 3.15.2

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.2: 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.

### 3.15.2: 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.
- Syntax highlighting did not work on the "Code" view of a file.
- After an initial reboot, the appliance sometimes altered the ownership permissions of `gitmon` directories. As a result, the Management Console got stuck 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, the `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.
- In some cases, `ghe-spokesctl status` (without `--live`) displayed entries that no longer existed.

## 3.15.2: Changes

- The 400GB root disk requirement introduced in Enterprise Server 3.15.0 has been reverted. The 400GB root disk size is no longer a requirement for GHES new installations and upgrades. Customers on standalone or standalone HA topologies are still recommended to upgrade their root disk size to 400GB.
- 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.

### 3.15.2: Closing down

- All users should be aware that GitHub Projects (classic) are closing down. They should migrate to new Projects powered by GitHub Issues. See Migrating from projects (classic).

  GitHub Projects (classic) will be retired in GitHub Enterprise Server 3.17. For more information, see the Projects (classic) sunset blog post.

### 3.15.2: 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.
- 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.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running ghe-cluster-repl-status if a new organization and repositories are created before using the ghe-cluster-repl-bootstrap command. To avoid this issue, complete the cluster HA setup with ghe-cluster-repl-bootstrap before creating new organizations and repositories.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

## 3.15.2: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.15.2, 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 3.15.1

Download GitHub Enterprise Server 3.15.1

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

### 3.15.1: Security fixes

- Packages have been updated to the latest security versions.
- **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]

### 3.15.1: 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.
- Preflight checks now recognize the updated 500GB user disk as a recommendation, not a requirement.
- 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.
- Customers performing a feature version upgrade to 3.13.6 or 3.14.3 could experience issues with database migrations due to data issues during database conversions.
- 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

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

### 3.15.1: Changes

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

### 3.15.1: Known issues

- Syntax highlighting does not work on the "Code" view of a file. This error will be fixed in the next release. [Updated: 2025-01-10]
- Admins setting up cluster high availability (HA) may encounter a `spokes` error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- 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.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- 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.

- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

### 3.15.1: Deprecations

- **Upcoming deprecation of projects (classic)**
  - Projects (classic) will be removed from GitHub Enterprise Server 3.16 and later. For more information, see Sunset Notice – Projects (classic).

### 3.15.1: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.15.1, 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 3.15.0

Download GitHub Enterprise Server 3.15.0

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.

---

> **Warning**: We received a few reports of performance issues with GitHub Enterprise Server versions 3.15, 3.16, and 3.17 and have shipped performance fixes to the affected versions. You can now upgrade to 3.15.12, 3.16.8, 3.17.5, or later. We do not recommend upgrading to earlier releases of 3.15, 3.16, or 3.17. [Updated: 2025-08-25]

## 3.15.0: Features

- **Instance administration**
  - New installations of GitHub Enterprise Server version 3.15 and upgrades to 3.15 now require a root disk size of at least 400GB. Otherwise, the system will not boot. For more information on how to increase the root disk size in the appliance, see Increasing storage capacity.
  - Minimum recommended requirements for vCPUs, memory, root storage, and data storage have been updated. See Installing GitHub Enterprise Server on VMware.

- **Audit logs**
  - Organization owners and security managers can monitor changes to the use of security configurations at the organization and repository levels. See About enabling security features at scale," `security_configuration`, and `repository_security_configuration`

- **Code scanning**
  - Users can run CodeQL analysis of C# code without building the project, `build-mode: none`. When you enable code scanning using default setup on a repository, both Java and C# use this mode. Analysis of both languages using this method is generally available. See About build mode None for CodeQL.
  - CodeQL analysis of Swift and Kotlin code is generally available.
  - This release comes installed with version **2.18.4** of the CodeQL CLI, used in the CodeQL action for code scanning. Significant updates since the default version installed on GitHub Enterprise Server 3.14 include:

    - Support for Go 1.23 and TypeScript 5.5
    - C# can now use `build-mode: none`, which allows scanning C# code without requiring working builds
    - Kotlin & Swift support for mobile applications is generally available
    - Java `build-mode: none` analyses only report a warning on the tool status page when significant analysis problems are detected
    - Two new JavaScript queries, `js/functionality-from-untrusted-domain`, have been added to detect usage of scripts from untrusted domains, including `polyfill.io` content delivery network and `js/insecure-helmet-configuration` to detect instances where important Helmet security features are disabled
    - The precision of `cpp/iterator-to-expired-container` & `cpp/unsafe-strncat` have been increased to high

- **Secret scanning**

    - Secret scanning for discussions, issues, and pull request titles, bodies, and comments is now generally available. See About secret scanning.
    - Users can bypass push protection using the existing `Create a blob` and `Create or update file contents` REST API endpoints. This action can also be performed programmatically using the new `Create a push protection bypass` API endpoint. See the GitHub Blog post.
    - Organization owners can enable the detection of non-provider patterns for their organization using a security configuration. This feature is in public beta and is subject to change. See Enabling detection of non-provider patterns for an organization.

- **Dependabot**

    - Organization owners, security managers and users with **admin** access can manage Dependabot auto-triage rules, as well as create custom auto-triage rules. Auto-triage rules are a powerful tool that automatically dismiss Dependabot alerts matching certain criteria. This feature is generally available. See About Dependabot auto-triage rules.

- **GitHub Connect**

    - For enterprises with a deployment of GitHub Enterprise Cloud on GHE.com, automatic license sync is supported from GitHub Enterprise Server to GHE.com.

- **GitHub Advanced Security**
  - Organization owners and security managers can use a "CodeQL pull request alerts" view in security overview to proactively identify and mitigate security risks at the organization and enterprise level. For example, they can see the most common alerts found in pull requests and see the corresponding remediation rates. See Viewing metrics for pull request alerts.

- **Code security**
  - Organization owners and security managers can simplify the rollout of GitHub security products at scale with security configurations. They can define collections of security settings, save them as a custom configuration, and apply them across groups of repositories. Security configurations can be enforced using policies to stop repositories making any changes to the enablement of security features. See About enabling security features at scale.
  - Organization owners and security managers can create, apply, enforce, and monitor security configurations programmatically using REST API calls and audit logs. See Configurations and `security_configuration`.

- **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 2.319.1. 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.

- **GitHub Packages**
  - Package managers benefit from improved performance as the npm registry no longer includes README content in package version metadata, reducing the size of package packuments (metadata manifest). This change enhances registry and npm CLI efficiency.

- **Repositories**
  - Users can use new property types when creating a custom property: `Multi select` and `True/False`. See Managing custom properties for repositories in your organization.

  - Users can gain deeper insights into contributors and code frequency with enhanced focus navigation, and a new table format for viewing and downloading data. See Enhanced Repo Insights Views on the GitHub Blog.
  - Users can require that merges must be performed with a merge queue at the repository level. See the GitHub blog post. For more information about merge queues, see Merging a pull request with a merge queue.
  - Admins can enforce status checks and workflow runs on existing refs while allowing the creation of new refs. See the GitHub blog post.
  - Organization members can use the new repository view and advanced filters to find repositories by visibility, language, custom properties, size, license, and more. See the GitHub blog post.

- **Projects**
  - Users can interact with project status updates programmatically using the `ProjectV2StatusUpdate` GraphQL object and the `projects_v2_status_update` webhook event. See GitHub Issues & Projects on the GitHub Blog.
  - For better accessibility, swimlanes and card titles have heading elements attached to them.
  - Project custom field changes are included directly in the project_v2_item webhook event when a project item's fields are edited, allowing users to understand how project fields change over time and how long they have a particular value. See GitHub Issues & Projects – GraphQL and webhook support for project status updates and more! on the GitHub Blog.

- **Accessibility**
  - Users can navigate and dismiss hovercards using keyboard shortcuts, enhancing accessibility. Additionally, a new setting allows users to disable all hovercards. See Keyboard Navigation Improvements for Hovercards on the GitHub Blog.
  - Math equations are rendered with standardized MathML, replacing custom HTML MathJax to enhance accessibility and security. While most users will see minimal changes, slight differences in font and alignment may occur.
  - The light and dark high contrast themes have been updated to improve readability. See High contrast theme improvements on the GitHub Blog.

- **Integrations and extensions**

  - The `client_id` field is included in all API responses that describe a GitHub App. This is part of a shift to use the client ID as the primary identifier for an app. See Client IDs are now included in App API responses on the GitHub Blog.

  - When users go through the device code flow for an OAuth app, such as the GitHub CLI, they are prompted to use an account picker if they have multiple accounts.

## 3.15.0: Changes

- The API endpoint for listing custom deployment rule integrations for an environment ( `GET /repos/{owner}/{repo}/environments/{environment_name}/deployment_protection_rules/apps` ) requires **"Administration" repository permissions (read)** for fine-grained tokens. Previously, the token required "Actions" repository permissions (read).

- Pushes that update over 5,000 branches no longer trigger webhooks or GitHub Actions workflows.

- Organization owners and security managers will see a new organization-level code security settings UI. In the organization settings sidebar, the **Code security and analysis** option has been replaced by an expanding **Code security** option. This contains new **Configurations** and **Global settings** options. See About enabling security features at scale.

## 3.15.0: Known issues

- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.

- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.

- 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 by running `/usr/local/share/enterprise/ghe-nomad-jobs queue /etc/nomad-jobs/mssql/mssql.hcl` .

- Admins setting up cluster high availability (HA) may encounter a `spokes` error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.

- 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.

- 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.

- On Azure instances, a failed pre-upgrade check due to insufficient user disk size can result in the Management Console displaying an `Internal Server Error`. To restore access to the Management Console, run `sudo rm /var/log/preflight-check-report.json` to remove the file. If enabled, the `automatic update checks` need to be disabled from the Management Console until user disk size is increased to minimum 500 GB. To increase the user disk size, see Increasing storage capacity.

- 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.

- Upgrading to this version from GHES 3.14.19 and higher will cause the upgrade to fail due to this version containing an older version of MySQL. To avoid this issue please upgrade to GHES 3.15.14 or higher.

  [Updated: 2025-11-24]

### 3.15.0: Closing down

- In GitHub Enterprise Server 3.16, tag protection rules will be migrated to a ruleset and the tag protection rule feature will no longer be available.
- In GitHub Enterprise Server 3.16, the `/explore` functionality, including the `Activity` and `Trending` pages, will be removed.
- We are closing down the API endpoints and parameters that complemented the old organization-level code security settings UI experience. These have been replaced by a new API for security configurations. See Configurations.

  The following things are scheduled for removal in GitHub Enterprise Server 3.16.

  - **Closing down:** The GET response for security product status in an organization: Get an organization is deprecated. This attribute will return inaccurate information.
  - **Closing down:** The PATCH functionality for security products to set a default status for new repos in an organization: Update an organization is deprecated. The PATCH operation will be ignored.
  - **Closing down:** The POST endpoint to enable or disable a security feature for all repositories in an organization: Enable or disable a security feature for an organization is deprecated. Using the POST operation may result in a code security configuration being unintentionally removed from a repository.

### 3.15.0: Retired

- The Management Console API has been removed. The Manage GHES API reached feature parity with the Management Console API in GitHub Enterprise Server version 3.12. For information about the Manage GHES API, see REST API endpoints for managing GitHub Enterprise Server.
- The option to "copy Storage settings from Actions" in the Management Console ("GitHub Packages" > "Packages Storage Settings") has been removed.

### 3.15.0: Errata

- These release notes previously indicated as a known issue that on GitHub Enterprise Server 3.15.0, 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]