



Enterprise Server 3.16.16

[Download GitHub Enterprise Server 3.16.16](#)

March 12, 2026

🚩 This is not the [latest release](#) of Enterprise Server. Please use the latest release for the latest security, performance, and bug fixes.

3.16.16: 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 could use the REST API endpoints `/search/commits` or `/search/issues` with a personal access token (classic) that lacks the `repo` scope to retrieve results from private or internal repositories by using the `repo:OWNER/REPO` qualifier. GitHub has requested CVE ID [CVE-2026-3582](#) 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](#).

3.16.16: 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.
- 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.
- On instances with GitHub Actions enabled, Actions workflow runs could be silently skipped when creating many issues rapidly via the API. Previously, some "issue opened" webhooks were processed before the new issue was saved to the database, causing the event to be dropped and the workflow not to start.
- 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.

3.16.16: 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.

3.16.16: 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 `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.
- 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.
- 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.
- In a cluster, the host running restore requires access to the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email means the comment is not added to the issue.
- 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.
- Audit log entries for pre-receive hooks that have been rejected may not be recorded.
- When applying an enterprise security configuration to all repositories (for example, enabling secret scanning or code scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.

Enterprise Server 3.16.15

[Download GitHub Enterprise Server 3.16.15](#)

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 3.16.15 has been unpublished due to mismatched Git versions between containers. Please use the most recent available patch release of 3.16. [Updated: 2026-03-13]

3.16.15: 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 could use the REST API endpoints `/search/commits` or `/search/issues` with a personal access token (classic) that lacks the `repo` scope to retrieve results from private or internal repositories by using the `repo:OWNER/REPO` qualifier. GitHub has requested CVE ID [CVE-2026-3582](#) 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](#).

3.16.15: 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.
- 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.
- On instances with GitHub Actions enabled, Actions workflow runs could be silently skipped when creating many issues rapidly via the API. Previously, some "issue opened" webhooks were processed before the new issue was saved to the database, causing the event to be dropped and the workflow not to start.
- 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.

3.16.15: 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.

3.16.15: 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. 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 `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-frontent` 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 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.

- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email means the comment is not added to the issue.
- 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.
- Audit log entries for pre-receive hooks that have been rejected may not be recorded.
- When applying an enterprise security configuration to all repositories (for example, enabling secret scanning or code scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.

Enterprise Server 3.16.14

February 10, 2026

[Download GitHub Enterprise Server 3.16.14](#)

 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.

3.16.14: 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`).

3.16.14: 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](#).

3.16.14: Bug fixes [↗](#)

- Running `ghe-config-apply` could fail if Redis experienced transient connectivity issues during the configuration process.
- When administrators would apply 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.
- 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.

3.16.14: 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.

3.16.14: 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.
- 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.

- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- Audit log entries for pre-receive hooks that have been rejected may not be recorded.
- When applying an enterprise security configuration to all repositories (for example, enabling Secret Scanning or Code Scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.

Enterprise Server 3.16.13

[Download GitHub Enterprise Server 3.16.13](#)

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.

3.16.13: Security fixes [↗](#)

- **HIGH:** An authenticated attacker with permission to configure webhooks could perform SSRF to access internal-only services on the instance, potentially disrupting background job processing.

Exploitation required webhook configuration privileges and the ability to craft valid service requests. GitHub has requested CVE ID [CVE-2026-1999](#) for this vulnerability, which was reported via the [GitHub Bug Bounty](#) program.

3.16.13: 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.
- After selecting "local storage" for migration storage in the Management Console, administrators would find that the setting appeared to be cleared when the settings page refreshed.
- 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.

3.16.13: 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.
- To help large instances run more efficiently, enterprise administrators can more easily opt out of the behavior where GitHub generates a rebase commit every time we check whether a pull request can be merged. This change consolidates prior handling of multiple repository rule variables and backend feature flags.

Now, if an administrator sets the instance's

`skip_rebase_commit_generation_from_rebase_merge_settings` configuration variable to `true`, the "Allow rebase merging" option in a repository's pull request settings becomes the source of truth for whether rebase commits are generated when mergeability is checked.

3.16.13: Known issues [↗](#)

- When applying an enterprise security configuration to all repositories (for example, enabling Secret Scanning or Code Scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.
- 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.
- 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.
- In a cluster, the host running restore requires access to the storage nodes via their private IPs.

- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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 3.16.12

[Download GitHub Enterprise Server 3.16.12](#)

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.

3.16.12: 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](#).

3.16.12: Bug fixes [↗](#)

- Add missing `nvme_core.io_timeout=240` kernel parameter to Azure GRUB configuration to ensure NVMe readiness.
- 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.

3.16.12: 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-frontent` 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 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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 3.16.11

[Download GitHub Enterprise Server 3.16.11](#)

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.

3.16.11: 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.

3.16.11: 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.

- When a pull request was closed and reopened, the `merge` ref was not recreated.
- Administrators who had upgraded to the previous patch release may have observed a significant increase in executions of the `SecurityOverviewAnalytics::UpdateFeatureStatusSummaryJob` job, causing background job queue saturation, service delays, reduced stability, and lower performance for environments using security overview analytics.
- Link previews did not appear in Slack conversations when messages were delivered through socket mode, affecting the visibility of linked GitHub content.
- Users who accessed GitHub Enterprise Server with Chromium-based browsers experienced slow logout performance.
- 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.

3.16.11: 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.
- `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]

3.16.11: 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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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 3.16.10

[Download GitHub Enterprise Server 3.16.10](#)

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.

3.16.10: 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.

3.16.10: 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.
- After an upgrade, administrators found that Elasticsearch allocation remained set to "none," causing subsequent upgrades to fail. Enterprise upgrades now correctly set allocation to "all" after configuration is applied, preventing upgrade blocks.
- 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.
- Creating an organization would fail with a 500 or validation error if a maximum lifetime policy for personal access tokens was set to less than 366 days in the enterprise settings.
- 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 with thousands of organizations and roles, opening the security overview page for an organization or any other organization-level pages accessible via the Security tab triggered inefficient database queries that could degrade performance for other users.

- Administrators who had upgraded to the previous patch release may have observed a significant increase in executions of the `SecurityOverviewAnalytics::UpdateFeatureStatusSummaryJob`, causing background job queue saturation, service delays, reduced stability, and lower performance for environments using security overview analytics.
- 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".
- The GitHub system user was not always properly set on startup, occasionally surfacing in authentication errors or failed secret scanning jobs in logs.

3.16.10: 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.
- Logging of configuration runs is improved with streamlined logging for different configuration phases. Phase-specific logs are written to both the main log file (`ghe-config.log`) and the console for better visibility.

3.16.10: 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.
- 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.
- In a cluster, the host running restore requires access to the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.

- 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 3.16.9

[Download GitHub Enterprise Server 3.16.9](#)

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.

3.16.9: Security fixes [↗](#)

- Packages have been updated to the latest security versions.

3.16.9: Bug fixes [↗](#)

- The Git service (`babeld`) could panic in some cases, causing it to become unresponsive.
- 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.
- When configuring primary and secondary NTP servers, only a hostname was expected. This prevented server options (see the [chronyd man page for options](#)) from being used which would cause `ghe-config-check` and `ghe-config-apply` to throw validation errors.

- When adding a new git data node in cluster environments, pre-receive hooks were not synchronized, causing missing hooks on the new node. Pre-receive hooks are now synced automatically when running `ghe-config-apply`.
- 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.
- Users were unable to use the "/" key to focus the search bar on pages where a file tree is displayed.
- When users pushed to forked repositories from the command line, the users received incorrect links for creating push protection bypass requests. The links referenced the parent repository instead of the forked repository.

3.16.9: 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.

3.16.9: 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.
- 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.


- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.8

[Download GitHub Enterprise Server 3.16.8](#)

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 3.16. You can now upgrade to version 3.16.8, but not to earlier releases of 3.16. 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](#).

3.16.8: Security fixes [↗](#)

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

3.16.8: 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).
- 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.
- 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`.
- Audit log entries for some Dependabot-related events were missing for administrators and security teams due to an outdated allowlist configuration.
- 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.
- After upgrading to 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]
- Site administrators experienced crashes in MySQL when running data backfills, such as during database maintenance or upgrades.

3.16.8: 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.
- 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.

3.16.8: 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`) 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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.


- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.7

[Download GitHub Enterprise Server 3.16.7](#)

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]

3.16.7: Security fixes

- The maintenance page in the Management Console did not include cross-site request forgery (CSRF) protection.
- Packages have been updated to the latest security versions.

3.16.7: Bug fixes

- On instances in a cluster configuration, builds of GitHub Pages sites timed out in GitHub Actions workflows.

- 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.
- In some scenarios, during an upgrade from GHES 3.14 to GHES 3.16 the `BackfillDefaultLegacyEnterpriseConfigurationsTransition` migration step could fail.
- Administrators and users could experience delays due to performance regressions affecting the background processing of notification jobs.

3.16.7: 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`.
- Events for adding or removing issues and pull requests from a project, or changing their status within a project, are now included in the items timeline alongside existing events. This update helps administrators and users more comprehensively track project-related activity.

3.16.7: 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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution.
- 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 or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.6

July 15, 2025

[Download GitHub Enterprise Server 3.16.6](#)

 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]

3.16.6: 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.

3.16.6: Bug fixes

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

3.16.6: 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.

3.16.6: Known issues

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-23]
- 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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- In some scenarios, upgrades from GHES 3.14.x to 3.16 can fail with a migration error. Running `ghe-single-config-apply` *should* allow the migration to proceed, and complete the upgrade. This will be fixed in GHES 3.16.7. To work around this issue, in your Enterprise's Code Security Settings, disable all security settings that apply to "new repositories". Once upgraded, create an Enterprise Security Configuration with your desired settings and set that configuration as the default for new repositories.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.5

[Download GitHub Enterprise Server 3.16.5](#)

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]

3.16.5: Security fixes [↗](#)

- Packages have been updated to the latest security versions.

3.16.5: 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.
- Users could not create or view secret scanning push protection bypass requests for forked repositories because bypass requests were incorrectly associated with the root repository rather than the fork. Forked repositories now support their own 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.

3.16.5: Changes [↗](#)

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

3.16.5: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- Applying a new GitHub Enterprise Server license using the Management Console can sometimes fail with an HTTP 500 error.
- 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-frontent` 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 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.4

[Download GitHub Enterprise Server 3.16.4](#)

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]

3.16.4: 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.

3.16.4: 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.
- On an instance with GitHub Actions disabled, status check icons failed to render on repository commit lists.
- When users clicked and held on search suggestions in the search bar, they were not taken to the correct location.
- 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.
- 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.
- After an appliance reboot, code scanning did not always trigger or process analyses.
- In some situations, the kafka-lite service could cause client timeouts when processing consumer group membership sessions and expirations. [Updated: 2025-07-14]

3.16.4: Changes

- Site administrators who test the Prometheus endpoint can now use 127.0.0.1 as a trusted IP address. Previously, only specific IPs were allowed for testing.
- 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.](#)

3.16.4: 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.

3.16.4: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- 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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, comments made on an issue via email are not added to the issue.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.3

[Download GitHub Enterprise Server 3.16.3](#)

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]

3.16.3: 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.

3.16.3: 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.
- A pre-receive hook could fail due to blocked system calls.

- After updating the TLS certificate from the Management Console, users encountered 502 errors when creating releases and uploading artifacts. Running `ghe-config-apply` did not resolve the issue, as the alambic service required a manual restart.
- The sidebar menu did not display on the "Retired namespaces" page on the site admin dashboard.
- When migrating from an instance with S3 on AWS Gov Cloud, an incorrect URL was generated.
- 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.
- The security configuration page returned a 404 error when a user deleted a reviewer without first removing them as a bypass reviewer in the secret protection push protection settings.
- On instances where vulnerability alerts were not configured, server usage metrics did not upload as expected.
- For instances with secret scanning disabled through `ghe-config`, navigating to the "Risk" page on the "Security" tab for the organization or enterprise level, resulted in a 500 error.
- 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.

3.16.3: 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.

3.16.3: 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]

3.16.3: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- 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 `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.
- 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.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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.
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]


3.16.3: 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 3.16.2

April 17, 2025

[Download GitHub Enterprise Server 3.16.2](#)

 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]

3.16.2: 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.
- **HIGH:** An attacker could exploit an improper neutralization of input vulnerability in GitHub's Markdown rendering to embed malicious HTML/CSS in math blocks `$$.. $$`, which allowed cross-site scripting. Exploitation required access to the target GitHub Enterprise Server instance and privileged user interaction with the malicious elements. To mitigate this issue, GitHub has disallowed math blocks to be escaped early by dollar signs and improved math-rendered content by ensuring we escape non-wrapped content. GitHub has requested [CVE-2025-3246](#) for this vulnerability, which was reported via the [GitHub Bug Bounty program](#).

3.16.2: Bug fixes

- 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.
- In very large enterprises, customers who made multiple API requests to get Dependabot alerts for their enterprise encountered performance issues with the GitHub API.
- 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`).
- Pruning unreachable Git objects on a single replica could cause increased CPU load due to many Git checksum recalculations.

- 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.
- Using the "Update a secret scanning alert" REST API endpoint (`PATCH /repos/{owner}/{repo}/secret-scanning/alerts/{alert_number}`) to change the resolution and resolution comment for a closed alert would return a `422` error.
- In some cases during an upgrade, GitHub Advanced Security migration `DelegatedBypassConfigurationNotNil` failed.
- On an instance with GitHub Advanced Security and code scanning enabled, existing code scanning alerts that referenced other code failed to load after an upgrade.

3.16.2: 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, squash and merge, or split the commits into multiple pull requests.
- The `spokesctl info` and `spokesctl repos` commands now also show wikis that are part of a network.

3.16.2: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- 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.
- 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.
- Some customers upgrading from 3.11.x or 3.12.x may experience a bug with the feature "Automatic update checks", filling the root disk with logs causing a system degradation. To prevent this, you can turn off the feature "[Enable automatic update check](#)" in the management console.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- Repository Cache Replicas return `Repository not found` when changes have been pushed to the Primary instance that have not yet synchronized to the Cache Replica. This issue can also occur in all previous patches of this release.
- The security risk page returns a 500 error when secret scanning is disabled. [Updated: 2025-04-25]
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

Enterprise Server 3.16.1

March 25, 2025

[Download GitHub Enterprise Server 3.16.1](#)

 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]

3.16.1: Security fixes

- Packages have been updated to the latest security versions.

3.16.1: 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.
- Restoring from a backup did not always apply the latest data from GitHub Actions. All GitHub Actions data is now restored with a backup.
- For instances in a high availability configuration, Elasticsearch indices were deleted on failover and when `ghe-repl-teardown REPLICCA_HOSTNAME` was run from the primary instance. All indices are recoverable except audit log indices, whose source of truth is Elasticsearch itself.
- On an instance with security product defaults set on organizations, users were unable to upgrade from versions earlier than 3.15 due to database migration failures.
- 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 due to inefficient DNS queries.
- 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 <REPLICCA_HOSTNAME>` from the primary instance.

3.16.1: 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>.

3.16.1: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- Upgrades to 3.16.1 may fail due to an error while migrating a secret scanning database. The `ghe-migrations` command output will include a `DelegatedBypassConfigurationNotNil` error. To recover, you can restore from a backup, fail over to a replica, or reach out to GitHub Support if you encounter this issue. [Updated: 2025-04-03]
- 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` on the appliance after at least one hour system uptime. [Updated: 2025-04-22]
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- 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.
- Some customers upgrading from 3.11.x or 3.12.x may experience a bug with the feature "Automatic update checks", filling the root disk with logs causing a system degradation. To prevent this, you can turn off the feature "[Enable automatic update check](#)" in the management console.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.

- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- 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 at least one hour system uptime. [Updated: 2025-04-22]
- 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.
- The security risk page returns a 500 error when secret scanning is disabled. [Updated: 2025-04-25]
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]


3.16.1: Errata [↗](#)

- Known issues incorrectly indicated that administrators could immediately run the `/usr/local/share/enterprise/ghe-es-search-repair` script after a restore to resolve indexing and collaborator access issues. In reality, this script must be run only after the system has been up for at least one hour. [Updated: 2025-04-22]

Enterprise Server 3.16.0

[Download GitHub Enterprise Server 3.16.0](#)

March 11, 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: Customers who have security products enabled by default at the organization level will experience issues when upgrading from 3.14 to 3.16.0. We recommend waiting for the next 3.16 patch to upgrade.

3.16.0: Features [↗](#)

• Instance administration

- We have optimized the monitor dashboard to help administrators quickly understand the operational health of the appliance at a glance. The newly added dashboard is concise and has actionable metrics. See [About the monitor dashboards](#).
- GitHub Enterprise Server has Prometheus metrics exporter in the appliance. This was dark-shipped in version 3.12 and the security posture was improved in 3.16. It simplifies the process of setting up an observability and monitoring pipeline that integrates with an external Prometheus installation. Prometheus-compatible metrics can be scraped directly from the appliance. See [Exporting and scraping Prometheus metrics](#).
- Organization owners can manage security responsibilities more flexibly with updates to the security manager role. The role can be assigned directly to individual users, in addition to teams, allowing more precise control over security responsibilities. Additionally, security manager assignments are managed under Settings - Organization roles, streamlining role configuration alongside other organizational roles. See [Managing security managers in your organization](#).
- `ghe-config-apply` applies configuration changes conditionally to the relevant, targeted and specific migrations only. As a result, you can expect less downtime and fewer errors while running `ghe-config-apply`. You can still choose to run `ghe-config-apply` unconditionally using this command: `ghe-config-apply -f`.
- 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]

• Dependabot

- Users can configure Dependabot to create pull requests to keep their repositories up to date with the .NET SDK latest version. When a new version is detected, Dependabot creates a pull request to update the `global.json` file to the new version. See [Configuring Dependabot version updates](#) and [Dependabot options reference](#).

• Security overview

- On the security overview dashboard, users can find a SAST vulnerabilities summary table that highlights the top 10 CodeQL and third-party open alerts by count, grouped by vulnerability type. This table helps teams prioritize remediation by showing the most widespread vulnerabilities across their codebase. The table is available for both organizations and enterprises in the Detection view. See [Viewing security insights](#).
- On the security overview dashboard, users can view Prevention metrics alongside Detection and Remediation metrics at both the organization and enterprise levels. See [the GitHub blog post](#).
- Users can export CSV data from the "CodeQL pull request alerts" view for an organization. This expansion of the data you can export from security overview makes it easier for you to integrate the data with external systems, craft custom reports, and archive security information. See [Viewing metrics for pull request alerts](#).
- On the security overview dashboard, accessibility enhancements improve how users interact with and understand code security insights. Updates include enhanced color contrast, full keyboard navigation, and better screen reader support, making security data more accessible to all users. See [Accessibility improvements for security overview](#) on the GitHub blog.

• 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 2.321.0. See the release notes for this version in the [actions/runner repository](#). If your instance uses ephemeral self-hosted runners and you've disabled automatic updates, you must upgrade your runners to this version of the Runner application before upgrading your instance to this GitHub Enterprise Server release.
- Users can see job level annotations above the GitHub Actions log view, improving the discoverability of annotations.
- Users can control where CodeQL security analysis runs by specifying any custom label for self-hosted runners in code scanning's default setup. This update removes the previous

restriction requiring the `code-scanning` label, allowing analysis to run on the desired machine(s). See [Improved support for labeled Actions runners in CodeQL code scanning](#) on the GitHub blog.

- The CI/CD Admin role is a pre-defined organization role. Organization owners and teams can delegate comprehensive CI/CD management to individuals without the need to maintain a custom role. See [Roles in an organization](#).
- Enterprise administrators can authenticate with region-specific OIDC endpoints for improved compliance and performance.

• Repositories

- Enterprise and organization administrators can configure policies to restrict the usage of deploy keys across all the repositories of their organizations, giving them more control and greater security over their deploy keys. See [Setting a personal access token policy for your organization](#).
- Enterprise owners are a bypass role in rulesets, which will allow further restrictions in rules bypassing.
- Custom repository properties have an “additional options” section that administrators can use to easily manage properties.
- Organization rulesets using custom properties include a link to the exact list of repositories targeted.
- Organization owners can allow users to set custom properties during repository creation. This ensures appropriate rules are enforced from the moment of creation and improves discoverability of new repositories. See [the GitHub blog post](#).

• Security advisories

- Users who report security advisories can use the new CVSS 4.0 schema to calculate a base vulnerability score. See [About the GitHub Advisory database](#).
- In the GitHub Advisory Database, users have access to an estimated probability that a vulnerability will be exploited over the next 30 days, calculated by the FIRST organization. This Exploit Prediction Scoring System (EPSS) score makes it easier for you to compare the risks of different vulnerabilities to your organization. See [About the GitHub Advisory database](#).

- **Code scanning**

- Advanced setup for CodeQL code scanning supports using an actions dependency cache instead of downloading dependencies from registries in every run. Users should update their workflows to use a dependency cache if access to registries is unreliable or slow. Using a dependency cache reduces the risk of losing alerts when third-party registries don't work well and may produce a small performance improvement. See [CodeQL code scanning for compiled languages](#).
- The CodeQL tools are available as a Zstandard archive with faster download and decompression times compared with the previous Gzipped archive.
 - The time taken to set up CodeQL analysis is reduced for default and advanced setup. No action is required by users of default and advanced setup to use the Zstandard archive, as the CodeQL action will automatically download the new archive.
 - People who use the CodeQL CLI can directly update their processes to download the new Zstandard archive. See [Setting up the CodeQL CLI](#).

- **Secret scanning**

- Repository administrators, organization owners, and security managers can specify which teams or roles have the ability to bypass push protection. These controls introduce a review and approval cycle for pushes containing secrets from all other contributors. This functionality is generally available and includes the following improvements over the preview:
 - Organization owners and security managers can define different groups of bypass reviewers for groups of repositories using security configurations. See [Creating a custom security configuration](#).
 - When defining bypass reviewers, organization owners and security managers have the flexibility of using a fine-grained permission, in addition to the existing role and team options. See [Enabling delegated bypass for push protection](#).
 - For blocked secrets, bypass reviewers see the branch and file path of the secret which makes it easier to triage bypass requests effectively. See [Managing requests to bypass push protection](#).
 - Users of the REST API, webhooks, and audit logs have access to additional fields which record details for approved bypass requests resulting in secret scanning alerts. See [Push protection bypass request details are included in the REST API, webhooks, and audit logs for secret scanning alerts](#) on the GitHub blog.

- Reviewers can add comments to push protection bypass requests in secret scanning. These comments help provide context, explaining the reasoning behind approving or denying a request. Requesters gain clarity on why their request was denied, and other reviewers can better understand why a request was approved or denied.
 - Secret scanning supports delegated bypass controls for repository file uploads from the browser. When enabled, users without bypass permissions must submit a request to approved reviewers before uploading a file containing a detected secret, reducing the risk of accidental exposure. See [About delegated bypass for push protection](#).
 - Automatic detection of non-provider patterns that help you uncover secrets outside of patterns tied to specific token issuers, like HTTP authentication headers, connection strings, and private keys, is generally available. This release includes the following improvement over the preview:
 - Users can find security alerts from non-provider patterns on the "Experimental" view of the repository "Secret scanning alerts" page for a repository, and in the security overview for an organization. The new name for the view more clearly communicates the status of the alerts than the old name of "Other".
 - Users who reopen a secret scanning alert manually have the option to add a comment explaining why the alert needs to be reopened. Any comments added will be visible in the alert UI, REST API, and webhooks, in the same way as for comments on dismissing an alert.
 - Users can use a new REST API endpoint to report on the scanning history for a repository which is useful for auditing scans and also for troubleshooting. See [Access a repository's secret scanning scan history with the REST API](#) on the GitHub blog.
- **Code security**
 - Enterprise owners can simplify and standardize the rollout of GitHub security products by creating security configurations at the enterprise-level. An enterprise configuration can be applied to repositories at the enterprise or the organization level. This gives you the option to enforce security features enterprise-wide, or to define configurations centrally but apply them locally using organization-level filtering to define a group of repositories. See [Code security configurations now available at the enterprise level](#) on the GitHub blog.
 - Organization owners and security managers can apply security configurations to archived repositories. This makes it simpler to roll out configurations without having to filter for archived repositories, and ensures features like Dependabot, code scanning, and secret scanning are automatically reapplied if a repository is unarchived. In addition, secret scanning runs on all repositories, including archived repositories, so if you add a new

custom pattern, archived repositories will be scanned for matches. See [Code security configurations now support archived repositories](#) on the GitHub blog.

- Organization owners and security managers with GitHub Advanced Security enabled have extra filtering options so they can select repositories based on the enablement or disablement of code security features. See [New advanced filters for code security configurations](#) on the GitHub blog.

- **Monitoring**

- Enterprise administrators can better monitor the health of the appliance with optimized dashboards that provide concise, actionable metrics. See [About the monitor dashboards](#).

- **GitHub Mobile**

- GitHub Mobile users can stay focused on important updates with Focused Notifications. This feature prioritizes notifications from the past 30 days, including items they've authored, direct mentions, and assigned tasks, helping reduce noise and improve productivity.

3.16.0: Security fixes [↗](#)

- **HIGH:** An attacker could access environment variables in the debug artifacts uploaded by the CodeQL action after a failed code scanning workflow run. This includes any secrets that were exposed to the workflow as environment variables. The attacker requires read access to the repository to access the debug artifact. Users who do not have debug logging enabled are unaffected. The impact to GitHub Enterprise Server users is limited to internal actors. To mitigate this issue, GitHub no longer logs the complete environment by default. GitHub has requested [CVE-2025-24362](#) for this vulnerability, which was reported via the [GitHub Bug Bounty program](#).

3.16.0: Changes [↗](#)

- The 400GB root disk requirement introduced in [Enterprise Server 3.15.0](#) has been reverted in 3.15.2. The 400GB root disk size is no longer a requirement for new GHES installations and upgrades. Customers on standalone or standalone HA topologies are still recommended to upgrade their root disk size to 400GB.
- When an enterprise requires two-factor authentication (2FA), members who do not use 2FA still retain membership even without 2FA, including occupying seats in the enterprise and

organizations. However, these users won't be able to access the enterprise resources until they enable 2FA on their account. See [Requiring two-factor authentication for an organization](#).

- The Debian and RedHat releases have been signed with a new GPG key. If you installed `gh` via our official package repositories, please update your keyring to the new key to continue verifying GitHub CLI releases. See the [GitHub blog post](#).
- 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+.
- Customers who have code scanning enabled may experience slower transitions when upgrading to version 3.16.0, due to changes in the data model that require data migration. We recommend testing this upgrade in a non-production environment first, as it could result in longer downtime than expected. [Updated: 2025-06-12]

3.16.0: Known issues [↗](#)

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- Instances with security products enabled by default at the organization level will experience issues while upgrading from 3.14 to 3.16.0. We recommend waiting for the next 3.16 patch to upgrade. If you instead upgrade from 3.14 to 3.15, then from 3.15 to 3.16.0, the upgrade will succeed. [Updated: 2025-03-17]
- 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 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.
- When restoring data originally backed up from an appliance with version 3.13 or greater, the Elasticsearch indices must be reindexed before the data will display. 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 displays 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.
- 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.
- Customers upgrading from 3.11.x or 3.12.x may experience a bug with the feature "Automatic update checks", which fills the root disk with logs causing a system degradation. To prevent this, turn off the feature "[Enable automatic update check](#)" in the management console.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- Commenting on an issue via email is not reflected on the issue in Azure.
- 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 primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.

- 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]

- The security risk page returns a 500 error when secret scanning is disabled. [Updated: 2025-04-25]
- Upgrading to this version from GHES 3.14.19 and higher or 3.15.14 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 3.16.10 or higher.

[Updated: 2025-11-24]

3.16.0: Closing down

- As of November 6, 2024, Dependabot no longer supports Composer version 1, which has reached its end-of-life. If you continue to use Composer version 1, Dependabot will be unable to create pull requests to update your dependencies. If this affects you, we recommend updating to a supported release of Composer. As of October 2024, the newest supported version of Composer is 2.8, and the long-term supported version is 2.2. View [Composer's official documentation](#) for more information about supported releases.
- In GitHub Enterprise Server 3.17, GitHub will migrate tag protection rules to a ruleset and the tag protection rule feature will no longer be available. Prior to upgrading to 3.17, you can use the [migration feature](#) to move your tag protection rules.
- In GitHub Enterprise Server 3.17, GitHub will be closing down the Docker registry for GitHub Packages in favor of the GitHub Container Registry, which supports Docker packages. All packages in the Docker registry will be deleted and cannot be fetched past the closing down date.
- In GitHub Enterprise Server 3.17, Dependabot will no longer support Python 3.8, which has reached its end-of-life. If you continue to use Python 3.8, Dependabot will not be able to create pull requests to update dependencies. If this affects you, we recommend updating to a

supported release of Python. As of February 2025, Python 3.13 is the newest supported release.

- In GitHub Enterprise Server 3.17, Dependabot will no longer support NPM version 6, which has reached its end-of-life. If you continue to use NPM version 6, Dependabot will be unable to create pull requests to update dependencies. If this affects you, we recommend updating to a supported release of NPM. As of December 2024, NPM 9 is the newest supported release.
- In GitHub Enterprise Server 3.17 and later, the field `cvss` for GitHub security advisories in the REST & GraphQL APIs will be closing down in favour of the new `cvss_severities` field.
- In GitHub Enterprise Server 3.17 and later, the Trending functionality under `/explore` will be removed. It was supposed to be removed in version 3.16.

3.16.0: Retired [↗](#)

- Team discussions have been removed from GitHub Enterprise Server. This feature was retired in 2023. See the [GitHub Blog post](#).
- In GitHub Enterprise Server 3.16, the Activity functionality under `/explore` is removed.
- GitHub no longer supports .NET 6 in GitHub Enterprise Server 3.16 and later.
- As of October 15th, 2024, you will no longer be able to enable or disable GitHub security features for repositories from the organization-level security coverage view. This feature has been retired and replaced with code security configurations for managing these settings. See the [GitHub blog post](#).

3.16.0: Errata [↗](#)

- The release notes previously mentioned GitHub App private key limits, which did not ship in 3.16 and will ship in 3.17. Similarly, PAT rotation policies were mentioned but will ship instead in 3.17. [Updated: 2025-03-21]
- The release notes previously did not mention VMware ESXi 8.0 support. [Updated: 2025-04-02]
- The release notes previously mentioned Dependabot support for `pnpm` workspace catalogs, which did not ship in 3.16 and will ship in 3.17. [Updated: 2025-05-08]
- Customers who have code scanning enabled may experience slower transitions when upgrading to version 3.16.0, due to changes in the data model that require data migration. We recommend testing this upgrade in a non-production environment first, as it could result in longer downtime than expected. [Updated: 2025-06-12]

Legal

© 2026 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)