**Enterprise Server 3.17 release notes**

# Enterprise Server 3.17.14

Download GitHub Enterprise Server 3.17.14

April 21, 2026

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

## 3.17.14: Security fixes

- **HIGH**: An attacker could gain unauthorized access to private repositories by abusing scoped user-to-server (`ghu_`) tokens after their associated GitHub App installation was revoked or deleted. In certain cases, the authorization layer could incorrectly fall back to a global installation context instead of rejecting the request, allowing the token to access resources outside its intended installation or repository scope. This issue could be chained with weaknesses in token revocation timing and SSH push attribution to obtain a victim-scoped token and read private repository contents without victim interaction. GitHub has requested CVE ID CVE-2026-5845 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker could extract sensitive environment variables from a GitHub Enterprise Server instance through a timing side-channel attack against the notebook rendering service. When private mode was disabled, the notebook viewer followed HTTP redirects without revalidating the destination host, enabling an unauthenticated Server-Side Request Forgery (SSRF) to internal services. By measuring response time differences, an attacker could infer secret values character by character. GitHub has requested CVE ID CVE-2026-5921 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: A Management Console administrator could inject shell metacharacters into configuration fields via the Management Console configuration API, leading to arbitrary command execution on the appliance as the admin OS user. GitHub has requested CVE ID CVE-2026-4821 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **HIGH**: An attacker with knowledge of a target application's registered OAuth callback URL could gain unauthorized access to user accounts by exploiting incorrect regular expression matching in callback URL validation. GitHub has requested CVE ID CVE-2026-4296 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **MEDIUM**: An attacker with permission to manage secret scanning push protection settings in one repository could add or remove delegated bypass reviewers in a different repository by exploiting an incorrect authorization check in the `/settings/security_analysis/bypass_reviewers` endpoints. Authorization was checked against the repository in the URL route, but the action was applied to a different repository specified in the request body. The impact is limited to assigning existing trusted users as bypass reviewers. GitHub has requested CVE ID CVE-2026-3307 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **MEDIUM**: An authenticated attacker could determine the names of private repositories by their numeric ID through the mobile upload policy API endpoint, which returned repository names in validation error messages without verifying the caller's access. GitHub has requested CVE ID CVE-2026-5512 for this vulnerability, which was reported via the GitHub Bug Bounty program.

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

## 3.17.14: Bug fixes

- Dependabot security update jobs failed silently when dependency groups with `applies-to: security-updates` were configured.

- After administrators installed or removed a custom certificate authority (CA) certificate with `ghe-ssl-ca-certificate-install`, Dependabot services continued using the previous CA store and could fail to connect to external registries that required the updated CA.

- On an instance with GitHub Actions enabled, diagnostic log files for storage connectivity checks did not persist to disk when site administrators clicked **Test storage settings** in the Management Console or ran `ghe-config-apply` to apply configuration changes. This made storage connection failures difficult to troubleshoot because logs were unavailable in support bundles.

- During initial setup of a new instance, site administrators saw an "Oops! A configuration run is already in progress" error message in the Management Console even though `ghe-config-`

`apply` had not been run.

- When Consul replication failed to start, a misleading error message `exit: check_consul_replication: numeric argument required` was emitted to `ghe-config.log`.
- Consul replication would sometimes fail to start and would repeatedly display an error message `WARNING: Consul KV Replication Error` before terminating.
- On instances with Dependabot enabled, hotpatch upgrades could lock the Nomad jobs queue.
- On instances with GitHub Actions enabled, workflows using `actions/github-script@v7` failed with an Internal Server Error during action resolution. In the previous GHES version, the bundled actions/github-script repository referenced a Git object that no longer existed, causing all workflows using `actions/github-script@v7` to fail.
- API consumers could not access secret scanning scan history for archived repositories, even when the organization had a GitHub Advanced Security license.
- When applying a hotpatch or running a configuration with `ghe-config-apply`, the configuration run could fail with `ERROR: Restoring CodeQL Action release tags` if internal Git services were not yet fully available. The error message `SpokesAPI::TwirpServerError: unavailable` appeared in logs.
- On instances connected to GitHub Enterprise Cloud with data residency, the "GitHub.com actions" setting appeared in the GitHub Connect configuration despite this feature not being available for data residency deployments.
- On instances with GitHub Actions enabled, errors appeared in logs related to missing Elasticsearch field mappings for workflow runs. The workflow run data included an `archived` field that was not defined in the Elasticsearch index mapping.
- The site admin bar displayed debugging information used by GitHub.
- Suspended users were listed in an organization's list of members.
- Migrations to GitHub Enterprise Server failed when the importer service tried to import a pull request review comment that referenced a garbage-collected commit. Now, these comments are skipped gracefully.
- The site admin "All organizations" report included soft-deleted organizations.
- Users with GitHub Advanced Security enabled received a 503 error when retrieving code scanning alerts via the API or in the UI due to inefficient database query execution.

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

### 3.17.14: Changes

- Administrators can now set `mysql.innodb-online-alter-log-max-size` with `ghe-config` so the value persists when a configuration is applied or upgraded.
- Administrators can configure the maximum number of concurrent HTTP/2 streams per connection for HAProxy. To set this value, use `ghe-config core.haproxy-h2-max-concurrent-streams VALUE` and run `ghe-config-apply`. Previously, this value was hardcoded to 100.
- To limit misleading error messages when the `mysql_exporter` and `sql_exporter` exporters try to connect to the database, both exporters use an IPv4 address.

### 3.17.14: Known issues

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

  As a workaround, you can enable Actions without OIDC, then enable OIDC **immediately** once the process completes. You should do this immediately because enabling OIDC will remove all access to existing Actions logs and artifacts.
- During an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.

- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- If a hotpatch upgrade requires the `haproxy-frontend` service to be restarted, the restart will hang if there are existing long-lived connections, such as browser web sockets or Git operations. No new connections will be accepted for up to 5 minutes. Any existing unfinished connections at this time will be disconnected.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- An organization-level code scanning configuration page is displayed on instances that do not use GitHub Advanced Security or code scanning.
- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- 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



and monitor system performance as you roll out changes.

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

## Enterprise Server 3.17.13

Download GitHub Enterprise Server 3.17.13

March 12, 2026

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

### 3.17.13: 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.

### 3.17.13: 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.
- For repositories using the Python uv package manager, `uv.lock` files were not included in the dependency graph. This prevented Dependabot from detecting vulnerable dependencies or providing security updates for those files.
- 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.

## 3.17.13: 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.

## 3.17.13: 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- 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 3.17.12

Download GitHub Enterprise Server 3.17.12

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 3.17.12 has been unpublished due to mismatched Git versions between containers. Please use the most recent available patch release of 3.17. [Updated: 2026-03-13]

## 3.17.12: 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.

## 3.17.12: 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.
- For repositories using the Python uv package manager, `uv.lock` files were not included in the dependency graph. This prevented Dependabot from detecting vulnerable dependencies or providing security updates for those files.
- 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 to not start. After this fix, workflow runs start reliably for all rapid issue creations, regardless of timing.
- 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.

### 3.17.12: 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.

### 3.17.12: 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 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 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- 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 3.17.11

Download GitHub Enterprise Server 3.17.11

February 10, 2026

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

---

## 3.17.11: 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` ).
- For administrators using geo-replication or high availability (HA), `ghe-repl` tooling supports cross-cluster replication (CCR) for Elasticsearch, improving search index replication between instances.

## 3.17.11: 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 attacker could merge their own pull request into a repository that allowed forks and for which they didn't have write access, by exploiting an incorrect authorization check in the `enable_auto_merge` mutation for pull requests in specific scenarios. Exploitation required a clean pull request status and only applied to branches without branch protection rules enabled. GitHub has requested CVE ID CVE-2026-1999 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.

### 3.17.11: Bug fixes

- Alambic failed to start after reboot or upgrade if legacy multi-disk for alambic was set up.

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

- When administrators configured password authentication, the Prometheus endpoint for OpenTelemetry metrics failed to expose metrics due to health check failures.

- 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.

- The GitHub Enterprise Server staffbar was displaying debugging information used by GitHub.

- 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.

### 3.17.11: 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.

- On high-availability clusters with Elasticsearch Cross Cluster Replication (CCR) enabled, replication failed if the datacenter and consul-datacenter values didn't match.
- The `spokesctl status` command displays the current priority of repository issues based on the most recent check. Previously, the command displayed the highest priority the issue had reached since it was first detected, which could be misleading if the issue had been partially resolved.

## 3.17.11: 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.

- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

- 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 3.17.10

Download GitHub Enterprise Server 3.17.10

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.

---

### 3.17.10: 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.

### 3.17.10: 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 found 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.
- Site administrators could not generate a CSV list of SCIM-provisioned users with the `ghe-scim-identities-csv` command because its wrapper script was missing from `/usr/local/bin`.
- Administrators encountered inaccurate free disk space calculations when setting Elasticsearch watermarks, as incorrect methods were used for determining root and data disk sizes.
- Upgrading an instance from 3.17.x or 3.18.x to 3.19.x would reset existing observability metrics settings.
- 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.

## 3.17.10: 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.

- Developers can see code scanning annotations listed with errors first, followed by warnings and notes, in newly generated annotation lists. Previously, annotation order was random, which could make critical issues less visible, especially when some annotations were omitted due to high alert volume. This improves the clarity and prioritization of code scanning results.

- 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.

## 3.17.10: 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

---

## Enterprise Server 3.17.9

Download GitHub Enterprise Server 3.17.9

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.

---

### 3.17.9: 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.

### 3.17.9: Bug fixes

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

### 3.17.9: 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 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

# Enterprise Server 3.17.8

Download GitHub Enterprise Server 3.17.8

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.

## 3.17.8: 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.

## 3.17.8: 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.

- Teams granted all-repository organization roles could not be requested as reviewers in pull requests.
- GraphQL queries using fine-grained tokens returned empty fields for organization members' public email addresses, while classic tokens provided expected results. All queries now receive that information, resolving inconsistency for integrations and reporting workflows that depend on member email data.
- Organization creation would fail with a 500 error when the system attempted to verify CAPTCHA responses even when no CAPTCHA challenge was presented to the user.
- An "Invite member" button intended only for GitHub.com was displayed on the enterprise "People" tab.
- 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.

## 3.17.8: Changes

- A new weekly job automatically disables Elasticsearch deprecation logging and removes existing deprecation logs every Saturday at midnight. This helps administrators manage disk

space by regularly cleaning up deprecation data streams and log indices that are no longer needed.

- Administrators can add security key-backed (SK) SSH certificate authorities.
- Administrators and users experience faster and more efficient searching of GitHub Actions workflow runs, with lower compute and networking resource usage. Searches for workflow runs within a repository are now always scoped to an associated repository.
- `ghe-repl-start` can now be executed without requiring a maintenance window when setting up a new replica, as long as `ghe-repl-setup` is immediately followed by `ghe-config-apply`. [Updated: 2025-12-17]

### 3.17.8: 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. 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error

from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

---

## Enterprise Server 3.17.7

Download GitHub Enterprise Server 3.17.7

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.

---

### 3.17.7: 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.

### 3.17.7: Bug fixes

- Initializing a cluster configuration for the first time could fail with `Error: Validation preflight-check`.
- 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.
- Users applying a new license file received an HTTP 500 error.
- 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 pull requests in organization-owned repositories, users could not request reviews from teams with the "All-repository read" organization role.
- Administrators experienced 500 errors when attempting to run Dependabot from the Security tab, to scan repositories for dependency vulnerabilities.
- 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.
- In rare cases, inconsistent data could lead to a panic in the code scanning service, causing it to restart and become unavailable for a few seconds. This could cause HTTP 500 errors when interacting with the code scanning API or in parts of the UI.

### 3.17.7: 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.

### 3.17.7: 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 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

---

## Enterprise Server 3.17.6

Download GitHub Enterprise Server 3.17.6

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.

---

### 3.17.6: Security fixes

- Packages have been updated to the latest security versions.

### 3.17.6: Bug fixes

- 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.
- After upgrading to 3.17.0, administrators encountered errors when using the `ghe-user-unsuspend` command-line utility to unsuspend users.
- 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.
- Users received an email for secret scanning alert dismissal requests if they had organization-level permission to review and manage dismissal requests, even if they lacked the necessary permission for the repository the request was for.

### 3.17.6: Changes

- Administrators can now invoke `ghe-storage-init-backup`, the backup initialization script introduced in 3.17, from any location as it is installed in the system PATH instead of the `/usr/local/share/enterprise` directory.
- 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.
- Azure VMs that use the NVMe disk controller are now supported, as well as Azure VMs that do not include temporary resource disks.
- Administrators and integrators who use release webhooks can track when assets are uploaded to or deleted from a release. The release webhook with the edited action triggers for asset changes, making it easier to audit asset updates.
- Webhook payloads for releases, pull request review threads, and pull request reviews include an `updated_at` field with the ISO8601 timestamp of the most recent modification. This makes it easier for integrators and other webhook consumers to track changes.

### 3.17.6: 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

  [Updated: 2025-11-24]

# Enterprise Server 3.17.5

Download GitHub Enterprise Server 3.17.5

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 3.17. You can now upgrade to version 3.17.5, but not to earlier releases of 3.17. 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.

## 3.17.5: 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.
- **LOW:** In repositories where delegated alert dismissal was enabled, requests to resolve a secret scanning alert using the REST API were accepted when the actor had insufficient permission. The endpoint checked to see if the actor had permission to resolve secret scanning alerts but failed to verify that the actor was also a valid reviewer. This could allow an actor to bypass the review process. The endpoint was updated to use the same logic as the UI.
- Elasticsearch packages have been updated to the 8.18.0 security version.
- Packages have been updated to the latest security versions.

## 3.17.5: 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. This is fixed for future enablement and upgrades.
- Site administrators observed that secondary database nodes, including those in replica clusters, were unnecessarily rebuilding indexes meant for the primary database during maintenance operations, leading to data redundancy in secondary databases.
- 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`.
- Organization administrators and integrators reviewing bypass requests using the API could not filter requests by the `approved` status.
- On instances configured for SAML authentication only, site administrators could not create new users via the API.
- 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.
- Audit log entries for some Dependabot-related events were missing for administrators and security teams due to an outdated allowlist configuration.
- After upgrading to 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.

### 3.17.5: 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 dont output transient Elasticsearch health check failures. This update reduces log verbosity to address confusion reported by users.

- Organization API responses included in migration workflows did not return all member privileges required by import APIs. Additional member privilege fields are now included in the organization hash when retrieving organization data via the API.
- 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.

### 3.17.5: 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.
- 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.
- 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`.

- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- 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 3.17 with caution.
- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

  [Updated: 2025-11-24]

# Enterprise Server 3.17.4

Download GitHub Enterprise Server 3.17.4

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]

## 3.17.4: 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.

## 3.17.4: Bug fixes

- When generating a support bundle, site administrators could encounter errors if character escaping caused the bundle script to omit the URL parameter for `curl`.
- 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.
- Taking a backup snapshot would sometimes fail because of a permissions error when the backup process attempted to create log files.
- 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.

- SCIM provisioning requests failed when a user's non-primary email was sent by the identity provider.
- SCIM managed enterprise users were able to edit email addresses.
- Administrators and users could experience delays due to performance regressions affecting the background processing of notification jobs.

### 3.17.4: 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.

### 3.17.4: 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.
- 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 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`.
- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- 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 3.17 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 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.17.3

Download GitHub Enterprise Server 3.17.3

July 15, 2025

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

---

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

### 3.17.3: 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.

### 3.17.3: Bug fixes

- Applying a new GitHub Enterprise Server license using the Management Console would sometimes fail with a HTTP 500 error.
- Users saw outdated references to delegated bypass for push protection being in public preview in the documentation for webhooks. Users may also have noticed unexpected behavior related to filtering newly approved push protection bypass requests on repository and organization request list pages.

### 3.17.3: 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.

### 3.17.3: 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 3.17 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.
- 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 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`.
- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

[Updated: 2025-11-24]

---

## Enterprise Server 3.17.2

Download GitHub Enterprise Server 3.17.2

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]

### 3.17.2: Security fixes

- **MEDIUM**: An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a user-to-server token with no scopes to disclose private repository names within an organization via Search API endpoint. This requires an organization admin to install a malicious GitHub App in the organizations repositories. GitHub has requested CVE ID CVE-2025-6600 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

### 3.17.2: 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.
- Repositories belonging to organizations with unbundled GitHub Advanced Security licenses did not receive webhooks for scan complete events.

- The secret scanning metrics page displayed data for expired delegated bypass requests.
- When users added a team with a repository role to the `CODEOWNERS` file, an unknown error was displayed. Teams with repository roles are now correctly recognized as valid owners of files.
- 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.
- In some cases, uploading a new license with unbundled GitHub Advanced Security did not fully unbundle all security configurations on the instance. Users saw errors such as "Advanced Security is not purchased" or "Validation failed: Secret scanning non provider patterns" when they tried to apply configurations to new repositories.

### 3.17.2: Changes

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

### 3.17.2: 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 3.17 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.
- 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 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`.
- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.17.1

Download GitHub Enterprise Server 3.17.1

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]

### 3.17.1: 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.

### 3.17.1: 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.
- Fixed an edge case for certain Security Configurations that would not automatically work when transitioning to unbundled GitHub Advanced Security SKUs.
- 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.
- On instances with dangling commit graph lock files, recompute checksum operations were unexpectedly triggered.
- 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]

### 3.17.1: 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.

### 3.17.1: 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.

### 3.17.1: 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 3.17 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.
- 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 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`.
- 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 to access the storage nodes via their private IP addresses.
- 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.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- Uploading a new license with unbundled GitHub Advanced Security may not fully unbundle all the Security Configurations on the instance in certain cases. Any active Security Configurations will continue to function, but when attempting to apply the configurations to new repositories

you may see errors like "Advanced Security is not purchased" or `Validation failed: Secret scanning non provider patterns. Non-provider patterns must be disabled when secret scanning is disabled`. Contact GitHub Support for assistance clearing this state in version 3.17.1. This issue will be resolved in version 3.17.2.

- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

  [Updated: 2025-11-24]

---

## Enterprise Server 3.17.0

Download GitHub Enterprise Server 3.17.0

June 03, 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]

### 3.17.0: Features

- **Instance administration**
  - During the upgrade to 3.17, the database transitions will be run concurrently. You may notice the upgrade taking less time.
  - GitHub Enterprise Server Backup Service is a managed backup solution built directly into the appliance. It provides simplified alternative to the `backup-utils`. The backup service is in public preview. See About the backup service for GitHub Enterprise Server.

- **Secret Protection and Code Security**
  - Users can secure code in their organizations and enterprises in an easier, more affordable, and scalable way to secure their code with the new standalone GitHub Advanced Security (GHAS) products: Secret Protection and Code Security. See Introducing GitHub Secret Protection and GitHub Code Security and GitHub Secret Protection and GitHub Code Security for GitHub Enterprise on the GitHub Blog.
    - Secret Protection is a security feature designed to detect and prevent the exposure of sensitive information, such as API keys, tokens, and passwords, in your code repositories. It includes tools like secret scanning, which identifies hardcoded secrets in your repositories, and push protection, which prevents developers from committing secrets to repositories in the first place. See Choosing GitHub Secret Protection
    - Code security is a security feature designed to help users identify, manage, and remediate vulnerabilities in their codebases, ensuring secure and compliant software development. It includes tools like code scanning, premium Dependabot features, and dependency review. See GitHub Code Security. Users on a GHAS subscription plans can transition at renewal time to a standalone subscription or a metered plan. Users on a Pay-as-You-Go plan can transition any time. See Billing models for Advanced Security products.

- **Secret Protection**
  - Organization owners can establish an approval process to control sensitive actions, such as restricting dismissal privileges of secret scanning alerts to designated individuals. This mitigates the risk of unauthorized changes and provides a documented record of bypass usage. See Delegated alert dismissal for code scanning and secret scanning now available in public preview on the GitHub Blog, and Establishing a governance framework for your enterprise.
  - Users can now access secret scanning scan events via the audit log and webhooks. Providing scan status visibility and reporting aims to enable users to independently diagnose unexpected scan behavior, as well as meet the auditing and compliance requirements of large enterprises by demonstrating scan activity. See Audit log and webhook events for secret scan completions on the GitHub Blog.
  - The detection of Base64-encoded GitHub tokens is now generally available, which means that users have better visibility into any leaked PATs. See Secret scanning detects Base64-encoded GitHub tokens on the GitHub Blog.

- The "Experimental" tab name for alerts, which caused confusion by leading certain users to underestimate the importance of its alerts, has been renamed "Generic". This tab includes alerts for non-provider patterns, which are not necessarily low confidence alerts. See Renaming secret scanning experimental alerts to generic alerts.

- Enterprises can manage push protection bypass requests for secret scanning via the REST API, enabling integration with existing workflows for reviewing and triaging. Reviewers can retrieve and act on bypass requests at the organization or repository level using new endpoints. This functionality supports delegated bypass controls, allowing only authorized users to bypass push protection, while others must submit requests for approval. See the GitHub Blog post.

- **Code Security**

  - Organization owners can establish an approval process to control sensitive actions, such as restricting dismissal privileges of code scanning alerts to designated individuals This mitigates the risk of unauthorized changes and provides a documented record of bypass usage. See Delegated alert dismissal for code scanning and secret scanning now available in public preview on the GitHub Blog, and Establishing a governance framework for your enterprise.

  - Users can access and search audit logs for code scanning-related events. These logs capture events impacting enterprises or organizations, including code scanning activities such as alert creation, resolution, reopening, or appearance in a new branch. See Code scanning now creates alert-related events in audit log on the GitHub Blog.

  - This release comes installed with version **2.20.7** of the CodeQL CLI, used in the CodeQL action for code scanning. Significant updates since the default version installed on GitHub Enterprise Server 3.16 include:

    - All experimental queries for C#, Java, and Kotlin have been promoted to the default query suite in the CodeQL community packs.
    - Full support for C# 13 and .NET 9, including coverage improvements to enhance alert detection and reduce false negatives.
    - Go 1.24 support, enabling analysis of the latest Go language features.
    - Java 24 support, with improvements to query accuracy for XSS and CSRF vulnerabilities.
    - JavaScript and TypeScript enhancements, including:
      - Optional response threat model to treat HTTP responses as tainted sources.
      - Improved precision for data flow through arrays and call resolution.
    - C/C++ improvements, including better accuracy for `cpp/static-buffer-overflow`.

- **Dependabot**
  - Users can automatically keep their `bun`, `Docker Compose`, and `uv` dependencies up to date with Dependabot version updates. See Supported ecosystems and repositories.
  - Users can use EPSS scores to help prioritize dependency vulnerabilities based on exploit likelihood. Using EPSS scores allows users to address vulnerabilities that are more likely to be exploited, reducing the risk of actual attacks. See Dependabot helps users focus on the most important alerts by including EPSS scores that indicate likelihood of exploitation, now generally available.
  - Developers using `pnpm` workspaces can ensure more reliable dependency updates with full Dependabot support for `pnpm` workspace catalogs. Dependabot prevents lockfile inconsistencies, avoids broken dependency trees, and improves update reliability in monorepos. See the GitHub blog post.

- **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 2.322.0. 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.

- **Identity and access management**
  - Automated user provisioning with the System for Cross-domain Identity Management (SCIM) standard is generally available. SCIM is a leading standard for user lifecycle management in SaaS applications. GitHub Enterprise Server instances using SAML authentication can enable SCIM to provision and manage user accounts from an identity provider (IdP). GitHub supports common integrations such as Entra ID and Okta, or you can use a custom SAML IdP and SCIM implementation to meet your organization's needs. You can configure SCIM using a supported IdP application or the SCIM REST API. See About user provisioning with SCIM on GitHub Enterprise Server.

- **Authentication**
  - Fine-grained personal access tokens (PATs) and PAT lifetime policies are now generally available. These tokens offer improved security with per-organization access, token

approval workflows, and better auditability through token ID tracking in audit logs. With lifetime policies you can also force the rotation of tokens on a configurable basis, helping drive down the use of long-lived PATs in your environment. See Fine-grained PATs are now generally available on the GitHub Blog.

- **Migrations**
  - Administrators can use the GHES Management Console to configure repository exports with local storage, reducing reliance on external blob storage and simplifying the migration process. Exports are stored on the GHES disk, and customers can choose how to provide the archive to GitHub Enterprise Importer, including using GitHub-owned blob storage.

- **Audit logs**
  - Audit log streaming of API requests targeting your enterprise's private assets is generally available.

- **Repositories**
  - Push rulesets are generally available. Users can block pushes to private and internal repositories, and their forks, based on file type, path, or size. Unlike pre-receive hooks, push rules are built-in, configurable via the UI or API, and support audit logs, evaluate mode, and bypass lists. See About rulesets.
  - Repository administrators can easily convert a fork into a standalone repository by leaving the fork network, which stops automatic syncing with the upstream repository. This is useful for taking a project in a new direction or maintaining separate versions.

- **Pull requests**
  - The refreshed pull request commits page is generally available. The updated page improves performance, aligns with GitHub's design system, and offers better accessibility.

- **Gist**
  - Users can moderate comments on gists by turning them off or deleting unwanted entries. See Moderating gist comments.

- **Commits**

  - Verified commits are attached to persistent verification records, allowing users to identify the first actor to introduce a commit to a repository. Users can rotate, expire, or revoke their signing key without impacting existing verifications.

    Verification records consume approximately 80 bytes on disk per signed commit. To limit data growth on large instances, site administrators can run `ghe-config app.persist-commit-signature-verification.enabled false` to disable persistent records.

- **GitHub Mobile**
  - GitHub Mobile users can quickly view their recent projects by clicking the Projects view from the Home screen.
  - GitHub Mobile supports additional functionality when connected to instances running GitHub Enterprise Server 3.17:
    - Compare branches: View and compare changes between branches directly from your mobile device.
    - Fork repositories: Fork public repositories in the mobile app.
    - Projects: Access and interact with GitHub Projects on the go.

- **Integrations and extensions**
  - GitHub App developers can improve security with a 25-key limit per app, encouraging safer key management practices. Apps exceeding the limit must delete excess keys before adding new ones. Additionally, scoped tokens can access more repositories. See Managing private keys for GitHub Apps.
  - Enterprise owners can centrally manage and share GitHub Apps across all organizations in their enterprise by creating enterprise-owned GitHub Apps. This eliminates the need to duplicate apps or make them `public`, reducing management overhead and improving security. `Private` and `internal` apps can be transferred to the enterprise level, with permission updates automatically applied across all organizations. Only `internal` visibility is supported, meaning only users and organizations within the enterprise can install and authorize these Apps. See Creating GitHub Apps for your enterprise.

## 3.17.0: Bug fixes

- Fetches from repository caches returned a "Repository not found" error when the cache is out of sync. [Updated: 2025-06-19]

## 3.17.0: Changes

- SAML response processing includes additional validation and schema checks. We recommend testing your SAML configuration on an upgraded staging appliance before upgrading your production appliance. See the SAML configuration guide for details on the required pieces of data, SAML configuration reference.
- Users see a horizontal navigation bar at the top of their enterprise account. This update is designed to improve the user experience by providing a consistent, intuitive navigation structure that mirrors the rest of the GitHub experience.

## 3.17.0: 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 3.17 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. See Troubleshooting access to the Management Console.
- 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`.
- 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 primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.
- Uploading a new license with unbundled GitHub Advanced Security may not fully unbundle all the Security Configurations on the instance in certain cases. Any active Security Configurations will continue to function, but when attempting to apply the configurations to new repositories you may see errors like "Advanced Security is not purchased" or `Validation failed: Secret scanning non provider patterns Non-provider patterns must be disabled when secret scanning is disabled`. Contact GitHub Support for assistance clearing this state in version 3.17.0. This issue will be resolved in version 3.17.2.
- Upgrading to this version from GHES 3.15.14 and higher or 3.16.10 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 3.17.7 or higher.

[Updated: 2025-11-24]

## 3.17.0: Closing down

- In GitHub Enterprise Server 3.20, GitHub will retire the security manager API in favor of the organization roles API. See the GitHub Blog.
- 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]

## 3.17.0: Retired

- Real-time job status updates for GitHub Actions workflow notifications in Slack and Microsoft Teams are no longer available. Users still receive notifications when a workflow starts and completes, but intermediate job progress updates have been removed to improve system efficiency.
- In GitHub Enterprise Server 3.17, tag protection rules will be migrated to a ruleset, and the tag protection rule feature will no longer be available.
- Dependabot is no longer supporting 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.
- Dependabot is no longer supporting 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.

## 3.17.0: Errata

- The "Features" section incorrectly indicated that updated insight views for repositories are available in this release. This feature is unavailable in GitHub Enterprise Server 3.17, and is available from GitHub Enterprise Server 3.19.0. [Updated: 2026-01-12]

## Legal

© 2026 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog