Enterprise Server 3.16.0

Download GitHub Enterprise Server 3.16.0

March 11, 2025

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

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

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

3.16.0: Features

- **Instance administration**
  - We have optimized the monitor dashboard to help administrators quickly understand the operational health of the appliance at a glance. The newly added dashboard is concise and has actionable metrics. See About the monitor dashboards.
  - GitHub Enterprise Server has Prometheus metrics exporter in the appliance. This was dark-shipped in version 3.12 and the security posture was improved in 3.16. It simplifies the process of setting up an observability and monitoring pipeline that integrates with an external Prometheus installation. Prometheus-compatible metrics can be scraped directly from the appliance. See Exporting and scraping Prometheus metrics.
  - Organization owners can manage security responsibilities more flexibly with updates to the security manager role. The role can be assigned directly to individual users, in addition to teams, allowing more precise control over security responsibilities. Additionally, security manager assignments are managed under Settings - Organization roles, streamlining role configuration alongside other organizational roles. See Managing security managers in your organization.
  - `ghe-config-apply` applies configuration changes conditionally to the relevant, targeted and specific migrations only. As a result, you can expect less downtime and fewer errors while running `ghe-config-apply`. You can still choose to run `ghe-config-apply` unconditionally using this command: `ghe-config-apply -f`.
  - Running GitHub Enterprise Server on the VMware ESXi 8.0 hypervisor is supported. If your installation is on VMware ESXi 7.x or earlier versions, you can now use the ESXi 8.0 hypervisor. [Updated: 2025-04-03]

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

- **Security overview**
  - On the security overview dashboard, users can find a SAST vulnerabilities summary table that highlights the top 10 CodeQL and third-party open alerts by count, grouped by vulnerability type. This table helps teams prioritize remediation by showing the most widespread vulnerabilities across their codebase. The table is available for both organizations and enterprises in the Detection view. See Viewing security insights.

    - On the security overview dashboard, users can view Prevention metrics alongside Detection and Remediation metrics at both the organization and enterprise levels. See the GitHub blog post.
    - Users can export CSV data from the "CodeQL pull request alerts" view for an organization. This expansion of the data you can export from security overview makes it easier for you to integrate the data with external systems, craft custom reports, and archive security information. See Viewing metrics for pull request alerts.
    - On the security overview dashboard, accessibility enhancements improve how users interact with and understand code security insights. Updates include enhanced color contrast, full keyboard navigation, and better screen reader support, making security data more accessible to all users. See Accessibility improvements for security overview on the GitHub blog.

- **GitHub Actions**
    - For self-hosted GitHub Actions runners on this GitHub Enterprise Server release, the minimum required version of the GitHub Actions Runner application is 2.321.0. See the release notes for this version in the `actions/runner` repository. If your instance uses ephemeral self-hosted runners and you've disabled automatic updates, you must upgrade your runners to this version of the Runner application before upgrading your instance to this GitHub Enterprise Server release.
    - Users can see job level annotations above the GitHub Actions log view, improving the discoverability of annotations.
    - Users can control where CodeQL security analysis runs by specifying any custom label for self-hosted runners in code scanning's default setup. This update removes the previous restriction requiring the `code-scanning` label, allowing analysis to run on the desired machine(s). See Improved support for labeled Actions runners in CodeQL code scanning on the GitHub blog.
    - The CI/CD Admin role is a pre-defined organization role. Organization owners and teams can delegate comprehensive CI/CD management to individuals without the need to maintain a custom role. See Roles in an organization.
    - Enterprise administrators can authenticate with region-specific OIDC endpoints for improved compliance and performance.

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

- **Security advisories**
    - Users who report security advisories can use the new CVSS 4.0 schema to calculate a base vulnerability score. See About the GitHub Advisory database.
    - In the GitHub Advisory Database, users have access to an estimated probability that a vulnerability will be exploited over the next 30 days, calculated by the FIRST organization.

This Exploit Prediction Scoring System (EPSS) score makes it easier for you to compare the risks of different vulnerabilities to your organization. See About the GitHub Advisory database.

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

- **Secret scanning**
  - Repository administrators, organization owners, and security managers can specify which teams or roles have the ability to bypass push protection. These controls introduce a review and approval cycle for pushes containing secrets from all other contributors. This functionality is generally available and includes the following improvements over the preview:
    - Organization owners and security managers can define different groups of bypass reviewers for groups of repositories using security configurations. See Creating a custom security configuration.
    - When defining bypass reviewers, organization owners and security managers have the flexibility of using a fine-grained permission, in addition to the existing role and team options. See Enabling delegated bypass for push protection.
    - For blocked secrets, bypass reviewers see the branch and file path of the secret which makes it easier to triage bypass requests effectively. See Managing requests to bypass push protection.
    - Users of the REST API, webhooks, and audit logs have access to additional fields which record details for approved bypass requests resulting in secret scanning alerts. See Push protection bypass request details are included in the REST API, webhooks, and audit logs for secret scanning alerts on the GitHub blog.
    - Reviewers can add comments to push protection bypass requests in secret scanning. These comments help provide context, explaining the reasoning behind approving or denying a request. Requesters gain clarity on why their request was denied, and other reviewers can better understand why a request was approved or denied.
    - Secret scanning supports delegated bypass controls for repository file uploads from the browser. When enabled, users without bypass permissions must submit a request to approved reviewers before uploading a file containing a detected secret, reducing the risk of accidental exposure. See About delegated bypass for push protection.
  - Automatic detection of non-provider patterns that help you uncover secrets outside of patterns tied to specific token issuers, like HTTP authentication headers, connection strings, and private keys, is generally available. This release includes the following improvement over the preview:
    - Users can find security alerts from non-provider patterns on the "Experimental" view of the repository "Secret scanning alerts" page for a repository, and in the security overview for an organization. The new name for the view more clearly communicates the status of the alerts than the old name of "Other".
  - Users who reopen a secret scanning alert manually have the option to add a comment explaining why the alert needs to be reopened. Any comments added will be visible in the alert UI, REST API, and webhooks, in the same way as for comments on dismissing an alert.

    - Users can use a new REST API endpoint to report on the scanning history for a repository which is useful for auditing scans and also for troubleshooting. See Access a repository's secret scanning scan history with the REST API on the GitHub blog.

- **Code security**
    - Enterprise owners can simplify and standardize the rollout of GitHub security products by creating security configurations at the enterprise-level. An enterprise configuration can be applied to repositories at the enterprise or the organization level. This gives you the option to enforce security features enterprise-wide, or to define configurations centrally but apply them locally using organization-level filtering to define a group of repositories. See Code security configurations now available at the enterprise level on the GitHub blog.
    - Organization owners and security managers can apply security configurations to archived repositories. This makes it simpler to roll out configurations without having to filter for archived repositories, and ensures features like Dependabot, code scanning, and secret scanning are automatically reapplied if a repository is unarchived. In addition, secret scanning runs on all repositories, including archived repositories, so if you add a new custom pattern, archived repositories will be scanned for matches. See Code security configurations now support archived repositories on the GitHub blog.
    - Organization owners and security managers with GitHub Advanced Security enabled have extra filtering options so they can select repositories based on the enablement or disablement of code security features. See New advanced filters for code security configurations on the GitHub blog.

- **Monitoring**
    - Enterprise administrators can better monitor the health of the appliance with optimized dashboards that provide concise, actionable metrics. See About the monitor dashboards.

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

3.16.0: Security fixes

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

3.16.0: Changes

- The 400GB root disk requirement introduced in Enterprise Server 3.15.0 has been reverted in 3.15.2. The 400GB root disk size is no longer a requirement for new GHES installations and upgrades. Customers on standalone or standalone HA topologies are still recommended to upgrade their root disk size to 400GB.
- When an enterprise requires two-factor authentication (2FA), members who do not use 2FA still retain membership even without 2FA, including occupying seats in the enterprise and organizations. However, these users won't be able to access the enterprise resources until they enable 2FA on their account. See Requiring two-factor authentication for an organization.
- The Debian and RedHat releases have been signed with a new GPG key. If you installed `gh` via our official package repositories, please update your keyring to the new key to continue verifying GitHub CLI releases. See the GitHub blog post.
- The CodeQL Action has been updated to v3.28.6 to enable uploading artifacts in debug mode without logging the complete environment when running CodeQL CLI v2.20.3+.

- Customers who have code scanning enabled may experience slower transitions when upgrading to version 3.16.0, due to changes in the data model that require data migration. We recommend testing this upgrade in a non-production environment first, as it could result in longer downtime than expected. [Updated: 2025-06-12]

3.16.0: Known issues

- Customers operating at high scale or near capacity may experience unexpected performance degradation, such as slow response times, background job queue spikes, elevated CPU usage, and increased MySQL load. Consider upgrading to 3.16 with caution. [Updated: 2025-07-28]
- Instances with security products enabled by default at the organization level will experience issues while upgrading from 3.14 to 3.16.0. We recommend waiting for the next 3.16 patch to upgrade. If you instead upgrade from 3.14 to 3.15, then from 3.15 to 3.16.0, the upgrade will succeed. [Updated: 2025-03-17]
- Custom firewall rules are removed during the upgrade process.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. See Troubleshooting access to the Management Console.
- On an instance with the HTTP `X-Forwarded-For` header configured for use behind a load balancer, all client IP addresses in the instance's audit log erroneously appear as 127.0.0.1.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the instructions for Replacing the primary database node, `ghe-cluster-config-apply` might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- When restoring data originally backed up from an appliance with version 3.13 or greater, the Elasticsearch indices must be reindexed before the data will display. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair .`
- An organization-level code scanning configuration page displays on instances that do not use GitHub Advanced Security or code scanning.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the ghe-cluster-repl-bootstrap command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- Customers upgrading from 3.11.x or 3.12.x may experience a bug with the feature "Automatic update checks", which fills the root disk with logs causing a system degradation. To prevent this, turn off the feature "Enable automatic update check" in the management console.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- Commenting on an issue via email is not reflected on the issue in Azure.

- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- For appliances in a high availability configuration, Elasticsearch indices are deleted in two situations:
  - On failover
  - When running `ghe-repl-teardown <REPLICA_HOSTNAME>` from the primary instance

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

  [Updated: 2025-03-19]
- The security risk page returns a 500 error when secret scanning is disabled. [Updated: 2025-04-25]

3.16.0: Closing down

- As of November 6, 2024, Dependabot no longer supports Composer version 1, which has reached its end-of-life. If you continue to use Composer version 1, Dependabot will be unable to create pull requests to update your dependencies. If this affects you, we recommend updating to a supported release of Composer. As of October 2024, the newest supported version of Composer is 2.8, and the long-term supported version is 2.2. View Composer's official documentation for more information about supported releases.
- In GitHub Enterprise Server 3.17, GitHub will migrate tag protection rules to a ruleset and the tag protection rule feature will no longer be available. Prior to upgrading to 3.17, you can use the migration feature to move your tag protection rules.
- In GitHub Enterprise Server 3.17, GitHub will deprecate the Docker registry for GitHub Packages in favor of the GitHub Container Registry, which supports Docker packages. All packages in the Docker registry will be deleted and cannot be fetched past the deprecation date.
- In GitHub Enterprise Server 3.17, Dependabot will no longer support Python 3.8, which has reached its end-of-life. If you continue to use Python 3.8, Dependabot will not be able to create pull requests to update dependencies. If this affects you, we recommend updating to a supported release of Python. As of February 2025, Python 3.13 is the newest supported release.
- In GitHub Enterprise Server 3.17, Dependabot will no longer support NPM version 6, which has reached its end-of-life. If you continue to use NPM version 6, Dependabot will be unable to create pull requests to update dependencies. If this affects you, we recommend updating to a supported release of NPM. As of December 2024, NPM 9 is the newest supported release.
- In GitHub Enterprise Server 3.17 and later, the field `cvss` for GitHub security advisories in the REST & GraphQL APIs will be deprecated in favour of the new `cvss_severities` field.
- In GitHub Enterprise Server 3.17 and later, the Trending functionality under /explore will be removed. It was supposed be removed in version 3.16.

3.16.0: Retired

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

3.16.0: Errata

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