

This version of GitHub Enterprise was discontinued on 2023-01-18. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, [upgrade to the latest version of GitHub Enterprise](#). For help with the upgrade, [contact GitHub Enterprise support](#).

Enterprise Server 3.3 release notes

Enterprise Server 3.3.19

[Download GitHub Enterprise Server 3.3.19](#)

January 17, 2023

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

Security fixes

- **HIGH:** Updated Git to include fixes from 2.39.1, which address [CVE-2022-41903](#) and [CVE-2022-23521](#).

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see "[Creating a support ticket](#)." [Updated: 2022-10-14]

Enterprise Server 3.3.18

[Download GitHub Enterprise Server 3.3.18](#)

January 12, 2023

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.

Security fixes

- Sanitize additional secrets in support bundles and the configuration log.
- Packages have been updated to the latest security versions.

Bug fixes

- The metrics `Active workers` and `Queued requests` for `github` (renamed from `metadata`), `githauth`, and `unicorn` container services weren't correctly read from `collectd` and displayed in the Management Console.

Changes

- The performance of configuration runs started with `ghe-config-apply` has been improved.
- When upgrading an instance with a new root partition, running the `ghe-upgrade` command with the `-t/--target` option ensures the preflight check for the minimum disk storage size is executed against the target partition.
- When exporting account data, backing up a repository, or performing a migration, the link to a repository archive now expires after 1 hour. Previously the archive link expired after 5 minutes.

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see "[Creating a support ticket](#)." [Updated: 2022-10-14]

Enterprise Server 3.3.17

December 13, 2022

[Download GitHub Enterprise Server 3.3.17](#)

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.

Security fixes

- **HIGH:** A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the instance. This vulnerability was reported via the [GitHub Bug Bounty Program](#) and has been assigned [CVE-2022-46256](#).
 - **HIGH:** An incorrect authorization vulnerability allowed a scoped user-to-server token to escalate to full admin access for a repository. An attacker would require an account with admin access to install a malicious GitHub App. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7.0. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2022-23741](#).
-

Bug fixes

- Installation of GitHub Enterprise Server on the VMware ESXi hypervisor failed due to the generation of an OVA file with an invalid capacity value.
 - When users performed an operation using the API, GitHub Enterprise Server enforced repository size quotas even when disabled globally.
 - A debug-level message appeared in a system log, which could consume space rapidly on the instance's root storage volume.
 - On instances where the dependency graph is enabled, upgrades could sometimes fail due to a slow-running migration of dependency graph data.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.

- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see "[Creating a support ticket](#)." [Updated: 2022-10-14]

Enterprise Server 3.3.16

[Download GitHub Enterprise Server 3.3.16](#)

November 22, 2022

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.

Security fixes

- **MEDIUM:** Updated [CommonMarker](#) to address a scenario where parallel requests to the Markdown REST API could result in unbounded resource exhaustion. This vulnerability has been assigned [CVE-2022-39209](#).
 - **MEDIUM:** Scoped user-to-server tokens from GitHub Apps could bypass authorization checks in GraphQL API requests when accessing non-repository resources. This vulnerability was reported via the [GitHub Bug Bounty Program](#) and has been assigned [CVE-2022-23739](#).
 - **MEDIUM:** Pull request preview links did not properly sanitize URLs, allowing a malicious user to embed dangerous links in the instances web UI. This vulnerability was reported via the [GitHub Bug Bounty program](#).
 - **MEDIUM:** An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a repository-scoped token with read/write access to modify GitHub Actions workflow files without a workflow scope. The "[Create or Update file contents API](#)" should enforce workflow scope. This vulnerability was reported via the [GitHub Bug Bounty program](#) and has been assigned [CVE-2022-46258](#).
-

Bug fixes

- Setting the maintenance mode with an IP Exception List would not persist across upgrades.
 - After configuration of Dependabot and alert digest emails, the instance would send digest emails to suspended users.
 - If a user configured a pre-receive hook for multiple repositories, the instances **Hooks** page would not always display the correct status for the hook.
 - Zombie processes no longer accumulate in the `gitrpcd` container.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see ["Creating a support ticket."](#) [Updated: 2022-10-14]

Enterprise Server 3.3.15

[Download GitHub Enterprise Server 3.3.15](#)

October 25, 2022

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.

Security fixes

- **HIGH:** Updated dependencies for the Management Console to the latest patch versions, which addresses security vulnerabilities including [CVE-2022-30123](#) and [CVE-2022-29181](#).
 - **HIGH:** Added checks to address an improper cache key vulnerability that allowed an unauthorized actor to access private repository files through a public repository. This vulnerability has been assigned [CVE-2022-23738](#).
 - **MEDIUM:** Updated [CommonMarker](#) to address a scenario where parallel requests to the Markdown REST API could result in unbounded resource exhaustion. This vulnerability has been assigned [CVE-2022-39209](#).
 - **MEDIUM:** Updated GitHub Actions runners to fix a bug that allowed environment variables in GitHub Actions jobs to escape the context of the variable and modify the invocation of `docker` commands directly. For more information, see the [Actions Runner security advisory](#).
 - **MEDIUM:** Updated Redis to 5.0.14 to address [CVE-2021-32672](#) and [CVE-2021-32762](#).
 - **MEDIUM:** An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2022-23737](#).
 - **LOW:** Due to a CSRF vulnerability, a `GET` request to the instance's `site/toggle_site_admin_and_employee_status` endpoint could toggle a user's site administrator status unknowingly.
 - Packages have been updated to the latest security versions.
-

Bug fixes

- After a site administrator made a change that triggered a configuration run, such as disabling GitHub Actions, validation of services would sometimes fail with the message `WARNING: Validation encountered a problem`.
 - After a site administrator installed a hotpatch containing changes to web interface assets such as JavaScript files or images, the instance did not serve the new assets.
 - Deleted assets and assets scheduled to be purged within a repository, such as LFS files, took too long to be cleaned up.
 - If a user installed a GitHub App for the user account and then converted the account into an organization, the app was not granted organization permissions.
-

Changes

- To ensure that site administrators can successfully complete an upgrade, the instance will now execute a preflight check to ensure that the virtual machine meets minimum hardware requirements. The check also verifies Elasticsearch's health. You can review the current requirements for CPU, memory, and storage for GitHub Enterprise Server in the "Minimum requirements" section within each article in "[Setting up a GitHub Enterprise Server instance](#)."
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see "[Creating a support ticket](#)." [Updated: 2022-10-14]

Enterprise Server 3.3.14

[Download GitHub Enterprise Server 3.3.14](#)

September 21, 2022

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.

Security fixes

- **HIGH:** A GitHub App could use a scoped user-to-server token to bypass user authorization logic and escalate privileges.
 - **MEDIUM:** The use of a Unicode right-to-left override character in the list of accessible files for a GitHub App could obscure additional files that the app could access.
 - Packages have been updated to the latest security versions.
-

Bug fixes

- Installation of a TLS certificate failed when the certificate's subject string included UTF-8 characters.
 - Configuration runs could fail when `retry-limit` or `retry-sleep-duration` were manually set by an administrator using `ghe-config`.
 - In some cases, the Management Console's monitor dashboard would not load correctly.
 - Removed a non-functional link for exporting Management Console monitor graphs as a PNG image.
 - When sending a support bundle to GitHub Enterprise Support using `ghe-support-upload`, the `-t` option would not successfully associate the uploaded bundle with the specified ticket.
 - A link back to the security settings for the instance's enterprise account could render an incorrect view.
 - Git clones or fetches over SSH could experience data corruption for transfers over 1GB in size.
 - After a user deleted or restored packages from the web interface, counts for packages could render incorrectly.
 - After successful configuration of Dependabot and alert digest emails, the instance would not send digest emails.
 - Manually disabled GitHub Actions workflows in a repository were re-enabled if the repository received a push containing more than 2048 commits, or if the repository's default branch changed.
 - When using a VPC endpoint URL as an AWS S3 URL for GitHub Packages, publication and installation of packages failed.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- Hotpatch upgrades to GitHub Enterprise Server may fail. Upgrades with the full `.pkg` are unaffected. If the upgrade fails for your instance, workaround this issue by connecting to the administrative shell (ssh) and running the following non-interactive command:

```
echo "grub-pc grub-pc/install_devices_empty boolean true" | sudo debconf-set-selections
```

If you're unable to upgrade, or if you need further assistance, contact GitHub Support. For more information, see "[Creating a support ticket](#)." [Updated: 2022-10-14]

Enterprise Server 3.3.13

August 30, 2022

[Download GitHub Enterprise Server 3.3.13](#)

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.

Bug fixes

- After unlocking a repository for temporary access, a site administrator was unable to manage settings for security products in the repository.
 - Duplicate administrative SSH keys could appear in both the Management Console and the `/home/admin/.ssh/authorized_keys` file.
 - In some cases, running `ghe-cluster-config-apply` could replicate an empty configuration to existing nodes in a cluster.
 - In some cases, configuration runs started with `ghe-config-apply` did not complete, or returned a `Container count mismatch` error.
 - After updating a self-signed TLS certificate on a GitHub Enterprise Server instance, UI elements on some pages in the web interface did not appear.
 - In some cases, background tasks could stall due to a library that was used concurrently despite not being thread-safe.
-

Changes

- Generation of support bundles is faster as a result of parallelized log sanitization. For more information about support bundles, see "[Providing data to GitHub Support](#)."
 - The enterprise audit log now includes more user-generated events, such as `project.create`. The REST API also returns additional user-generated events, such as `repo.create`. For more information, see "[Accessing the audit log for your enterprise](#)" and "[Using the audit log API for your enterprise](#)."
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.

- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.12

[Download GitHub Enterprise Server 3.3.12](#)

August 11, 2022

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.

Security fixes

- **CRITICAL:** GitHub Enterprise Server's Elasticsearch container used a version of OpenJDK 8 that was vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. The vulnerability is tracked as [CVE-2022-34169](#).
- **HIGH:** Previously installed apps on user accounts were automatically granted permission to access an organization on scoped access tokens after the user account was transformed into an organization account. This vulnerability was reported via the [GitHub Bug Bounty program](#).

Bug fixes

- When a custom dormancy threshold was set for the instance, suspending all dormant users did not reliably respect the threshold. For more information about dormancy, see "[Managing dormant users](#)."

Changes

- The enterprise audit log now includes more user-generated events, such as `project.create`. The REST API also returns additional user-generated events, such as `repo.create`. For more information, see "[Accessing the audit log for your enterprise](#)" and "[Using the audit log API for your enterprise](#)."

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

- The [file finder](#) does not return any results. To restore functionality, reinstall the 3.3.12 patch release using a full upgrade package. For more information, see "[Upgrading GitHub Enterprise Server](#)."

Enterprise Server 3.3.11

[Download GitHub Enterprise Server 3.3.11](#)

July 21, 2022

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.

Security fixes

- **MEDIUM:** Prevents an attack where a server-side request forgery (SSRF) could potentially force the Subversion (SVN) bridge to execute remote code by injecting arbitrary data into Memcached.
 - **MEDIUM:** Prevents an attacker from executing Javascript code by exploiting a cross-site scripting (XSS) vulnerability in dropdown UI elements within the GitHub Enterprise Server web interface.
 - Updates Grafana to version 7.5.16, which addresses various security vulnerabilities including [CVE-2020-13379](#) and [CVE-2022-21702](#).
 - Packages have been updated to the latest security versions.
 - **MEDIUM:** A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2022-23733](#). [Updated: 2022-07-31]
 - **MEDIUM:** A vulnerability involving deserialization of untrusted data was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the Subversion (SVN) bridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2022-23734](#).
-

Bug fixes

- Fixed an issue where the files inside the artifact zip archives had permissions of 000 when unpacked using an unzip tool. Now the files will have the permissions set to 644, the same way as it works in GitHub.com.
 - In some cases, the collectd daemon could consume excess memory.
 - In some cases, backups of rotated log files could accumulate and consume excess storage.
 - After an upgrade to a new feature release and subsequent configuration run, Elasticsearch could log excessive exceptions while rebuilding indices.
 - In some cases where a protected branch required more than one approving review, a pull request could be merged with fewer than the required number of approving reviews.
 - On instances using LDAP authentication, the authentication prompt for sudo mode incorrectly placed the cursor within the password field by default when text fields for both a username and password were visible.
-

Changes

- The `ghe-set-password` command-line utility starts required services automatically when the instance is booted in recovery mode.
 - Metrics for `aqueduct` background processes are gathered for Collectd forwarding and display in the Management Console.
 - The location of the database migration and configuration run log, `/data/user/common/ghe-config.log`, is now displayed on the page that details a migration in progress.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.10

[Download GitHub Enterprise Server 3.3.10](#)

June 28, 2022

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.

Security fixes

- **MEDIUM:** Ensures that `github.company.com` and `github-company.com` are not evaluated by internal services as identical hostnames, preventing a potential server-side security forgery (SSRF) attack.
- **LOW:** An attacker could access the Management Console with a path traversal attack via HTTP even if external

firewall rules blocked HTTP access.

- Packages have been updated to the latest security versions.

Bug fixes

- In some cases, site administrators were not automatically added as enterprise owners.
- After merging a branch into the default branch, the "History" link for a file would still link to the previous branch instead of the target branch.

Changes

- Creating or updating check runs or check suites could return `500 Internal Server Error` if the value for certain fields, like the name, was too long.

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.9

[Download GitHub Enterprise Server 3.3.9](#)

June 09, 2022

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.

Security fixes

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

Bug fixes

- An internal script to validate hostnames in the GitHub Enterprise Server configuration file would return an error if the hostname string started with a "." (period character).
 - In HA configurations where the primary node's hostname was longer than 60 characters, MySQL would fail to be configured
 - The `--gateway` argument was added to the `ghe-setup-network` command, to allow passing the gateway address when configuring network settings using the command line.
 - Image attachments that were deleted would return a `500 Internal Server Error` instead of a `404 Not Found` error.
 - The calculation of "maximum committers across entire instance" reported in the site admin dashboard was incorrect.
 - An incorrect database entry for repository replicas caused database corruption when performing a restore using GitHub Enterprise Server Backup Utilities.
-

Changes

- Optimised the inclusion of metrics when generating a cluster support bundle.
- In HA configurations where Elasticsearch reported a valid yellow status, changes introduced in a previous fix would block the `ghe-repl-stop` command and not allow replication to be stopped. Using `ghe-repo-stop --force` will now force Elasticsearch to stop when the service is in a normal or valid yellow status.
- When using `ghe-migrator` or exporting from GitHub.com, migrations would fail to export pull request attachments.

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.8

May 17, 2022

[Download GitHub Enterprise Server 3.3.8](#)

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.

Security fixes

- **MEDIUM:** A security issue in nginx resolver was identified, where an attacker who could forge UDP packets from the DNS server could cause 1-byte memory overwrite, resulting in worker process crashes or other potentially damaging impacts. The vulnerability has been assigned [CVE-2021-23017](#).

- Updated the `actions/checkout@v2` and `actions/checkout@v3` actions to address new vulnerabilities announced in the [Git security enforcement blog post](#).
 - Packages have been updated to the latest security versions.
-

Bug fixes

- In some cluster topologies, the `ghe-cluster-status` command left behind empty directories in `/tmp`.
 - SNMP incorrectly logged a high number of `Cannot statfs` error messages to syslog
 - For instances configured with SAML authentication and built-in fallback enabled, built-in users would get stuck in a “login” loop when attempting to sign in from the page generated after logging out.
 - Attempts to view the `git fsck` output from the `/stafftools/repositories/:owner/:repo/disk` page would fail with a `500 Internal Server Error`.
 - When using SAML encrypted assertions, some assertions were not correctly marking SSH keys as verified.
 - Videos uploaded to issue comments would not be rendered properly.
 - When using the file finder on a repository page, typing the backspace key within the search field would result in search results being listed multiple times and cause rendering problems.
 - When using GitHub Enterprise Importer to import a repository, some issues would fail to import due to incorrectly configured project timeline events.
 - When using `ghe-migrator`, a migration would fail to import video file attachments in issues and pull requests.
 - The Releases page would return a 500 error when the repository has tags that contain non-ASCII characters.
[Updated: 2022-06-10]
-

Changes

- In high availability configurations, clarify that the replication overview page in the Management Console only displays the current replication configuration, not the current replication status.
 - When enabling GitHub Packages, clarify that using a Shared Access Signature (SAS) token as connection string is not currently supported.
 - Support bundles now include the row count of tables stored in MySQL.
 - When determining which repository networks to schedule maintenance on, we no longer count the size of unreachable objects.
 - The `run_started_at` response field is now included in the [Workflow runs API](#) and the `workflow_run` event webhook payload.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.7

[Download GitHub Enterprise Server 3.3.7](#)

April 20, 2022

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.

Security fixes

- Packages have been updated to the latest security versions.

Bug fixes

- When a manifest file was deleted from a repository, the manifest would not be removed from the repository's

"Dependency graph" page.

- Resolved a regression that could lead to consistent failures to retrieve artifacts and download log archives for GitHub Actions. In some circumstances we stopped resolving URLs for internal communications that used `localhost`, and instead incorrectly used the instance hostname.
 - Upgrading the nodes in a high availability pair with an upgrade package could cause Elasticsearch to enter an inconsistent state in some cases.
 - Rotated log files with the extension `.backup` would accumulate in directories containing system logs.
 - In some cluster topologies, the command line utilities `ghe-spokesctl` and `ghe-btop` failed to run.
 - Elasticsearch indices could be duplicated during a package upgrade, due to an `elasticsearch-upgrade` service running multiple times in parallel.
 - In the pull request and commit views, rich diffs would fail to load for some files tracked by Git LFS.
 - When converting a user account to an organization, if the user account was an owner of the GitHub Enterprise Server enterprise account, the converted organization would incorrectly appear in the enterprise owner list.
 - Creating an impersonation OAuth token using the Enterprise Administration REST API resulted in an error when an integration matching the OAuth Application ID already existed.
 - The Secret Scanning REST API would return a `500` response code when there were UTF8 characters present in a detected secret.
 - Repository cache servers could serve data from non-cache locations even when the data was available in the local cache location.
-

Changes

- Configuration errors that halt a config apply run are now output to the terminal in addition to the configuration log.
 - When attempting to cache a value larger than the maximum allowed in Memcached, an error was raised however the key was not reported.
 - If GitHub Advanced Security features are enabled on your instance, the performance of background jobs has improved when processing batches for repository contributions.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories

are not included in GitHub.com search results.

- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.6

[Download GitHub Enterprise Server 3.3.6](#)

April 04, 2022

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.

Security fixes

- MEDIUM: A path traversal vulnerability was identified in GitHub Enterprise Server Management Console that allowed the bypass of CSRF protections. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.5 and was fixed in versions 3.1.19, 3.2.11, 3.3.6, 3.4.1. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned CVE-2022-23732.
- MEDIUM: An integer overflow vulnerability was identified in the 1.x branch and the 2.x branch of `yajil` which leads to subsequent heap memory corruption when dealing with large (~2GB) inputs. This vulnerability was reported internally and has been assigned CVE-2022-24795.
- Support bundles could include sensitive files if GitHub Actions was enabled.
- Packages have been updated to the latest security versions.

Bug fixes

- When enabling Dependabot, an error caused some security advisories to temporarily read as no-longer applicable.
 - Minio processes would have high CPU usage if an old configuration option was present after upgrading GitHub Enterprise Server.
 - The options to enable `TLS 1.0` and `TLS 1.1` in the Privacy settings of the Management Console were shown, although removal of those protocol versions occurred in an earlier release.
 - In a HA environment, configuring MSSQL replication could require additional manual steps after enabling GitHub Actions for the first time.
 - A subset of internal configuration files are more reliably updated after a hotpatch.
 - The `ghe-run-migrations` script would sometimes fail to generate temporary certificate names correctly.
 - In a cluster environment, Git LFS operations could fail with failed internal API calls that crossed multiple web nodes.
 - Pre-receive hooks that used `gpg --import` timed out due to insufficient `syscall` privileges.
 - In some cluster topologies, webhook delivery information was not available.
 - Elasticsearch health checks would not allow a yellow cluster status when running migrations.
 - Repositories would display a non-functional Discussions tab in the web UI.
 - Organizations created as a result of a user transforming their user account into an organization were not added to the global enterprise account.
 - Links to inaccessible pages were removed.
 - The GitHub Actions deployment graph would display an error when rendering a pending job.
 - Some instances experienced high CPU usage due to large amounts unnecessary background jobs being queued.
 - LDAP user sync jobs would fail when trying to sync GPG keys that had been synced previously.
 - Following a link to a pull request from the users Pull Request dashboard would result in the repository header not loading.
 - Adding a team as a reviewer to a pull request would sometimes show the incorrect number of members on that team.
 - The remove team membership API endpoint would respond with an error when attempting to remove member externally managed via a SCIM Group.
 - A large number of dormant users could cause a GitHub Connect configuration to fail.
 - The "Feature & beta enrollments" page in the Site admin web UI was incorrectly available.
 - The "Site admin mode" link in the site footer did not change state when clicked.
 - The `spokesctl cache-policy rm` command no longer fails with the message `error: failed to delete cache policy`.
-

Changes

- Memcached connection limits were increased to better accommodate large cluster topologies.
- The Dependency Graph API previously ran with a statically defined port.
- The default shard counts for cluster-related Elasticsearch shard settings have been updated.
- When filtering enterprise members by organization role on the "People" page, the text for the dropdown menu items has been improved.

- The “Triage” and “Maintain” team roles are preserved during repository migrations.
 - Performance has been improved for web requests made by enterprise owners.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.5

March 01, 2022

[Download GitHub Enterprise Server 3.3.5](#)

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.

Security fixes

- **HIGH:** An integer overflow vulnerability was identified in GitHub's markdown parser that could potentially lead to information leaks and RCE. This vulnerability was reported through the GitHub Bug Bounty program by Felix Wilhelm of Google's Project Zero and has been assigned CVE-2022-24724.
-

Bug fixes

- Upgrades could sometimes fail if a high-availability replica's clock was out of sync with the primary.
 - OAuth Applications created after September 1st, 2020 were not able to use the [Check an Authorization](#) API endpoint.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.4

[Download GitHub Enterprise Server 3.3.4](#)

February 17, 2022

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.

Security fixes

- It was possible for a user to register a user or organization named "saml".
 - Packages have been updated to the latest security versions.
-

Bug fixes

- GitHub Packages storage settings could not be validated and saved in the Management Console when Azure Blob Storage was used.
 - The mssql.backup.cadence configuration option failed ghe-config-check with an invalid charset warning.
 - Fixes SystemStackError (stack too deep) when getting more than 2^{16} keys from memcached.
 - A number of select menus across the site rendered incorrectly and were not functional.
-

Changes

- Dependency Graph can now be enabled without vulnerability data, allowing customers to see what dependencies are in use and at what versions. Enabling Dependency Graph without enabling GitHub Connect will *not* provide vulnerability information.
 - Secret scanning will skip scanning ZIP and other archive files for secrets.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.

- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.3

[Download GitHub Enterprise Server 3.3.3](#)

February 01, 2022

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.

Security fixes

- **MEDIUM:** Secret Scanning API calls could return alerts for repositories outside the scope of the request.
- Packages have been updated to the latest security versions.

Bug fixes

- Pages would become unavailable following a MySQL secret rotation until `nginx` was manually restarted.
- Migrations could fail when GitHub Actions was enabled.
- When setting the maintenance schedule with a ISO 8601 date, the actual scheduled time wouldn't match due to the timezone not being transformed to UTC.

- Spurious error messages concerning the `cloud-config.service` would be output to the console.
 - The version number would not be correctly updated after installing a hotpatch using `ghe-cluster-each`.
 - Webhook table cleanup jobs could run simultaneously, causing resource contention and increasing job run time.
 - When run from the primary, `ghe-repl-teardown` on a replica would not remove the replica from the MSSQL availability group.
 - The ability to limit email-based notifications to users with emails on a verified or approved domain did not work correctly.
 - When using CAS authentication and the "Reactivate suspended users" option was enabled, suspended users were not automatically reactivated.
 - A long-running database migration related to Security Alert settings could delay upgrade completion.
-

Changes

- The GitHub Connect data connection record now includes a count of the number of active and dormant users and the configured dormancy period.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible,

do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.2

[Download GitHub Enterprise Server 3.3.2](#)

January 18, 2022

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.

Security fixes

- Packages have been updated to the latest security versions. In these updates, Log4j has been updated to version 2.17.1. Note: previous mitigations released in 3.3.1, 3.2.6, 3.1.14, and 3.0.22 are sufficient to address the impact of CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832 in these versions of GitHub Enterprise Server.
 - Sanitize more secrets in the generated support bundles
 - Users on teams with the Security Manager role will now be notified about security alerts for repositories they are watching.
 - The security managers component will show a less-aggressive warning once the maximum number of teams has been reached.
 - The repository manage access page should return 403 when attempting to remove a security manager team from the repository.
 - Packages have been updated to the latest security versions.
-

Bug fixes

- Actions self hosted runners would fail to self-update or run new jobs after upgrading from an older GHES installation.
- Storage settings could not be validated when configuring MinIO as blob storage for GitHub Packages.
- GitHub Actions storage settings could not be validated and saved in the Management Console when "Force Path Style" was selected.
- Actions would be left in a stopped state after an update with maintenance mode set.
- Running `ghe-config-apply` could sometimes fail because of permission issues in `/data/user/tmp/pages`.
- The save button in management console was unreachable by scrolling in lower resolution browsers.

- IOPS and Storage Traffic monitoring graphs were not updating after collected version upgrade.
 - Some webhook related jobs could generated large amount of logs.
 - A Billing navigation item was visible in the site admin pages.
 - Several documentation links resulted in a 404 Not Found error.
-

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.1

December 13, 2021

[Download GitHub Enterprise Server 3.3.1](#)

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

Security fixes

- **⚠ Critical:** A remote code execution vulnerability in the Log4j library, identified as [CVE-2021-44228](#), affected all versions of GitHub Enterprise Server prior to 3.3.1. The Log4j library is used in an open source service running on the GitHub Enterprise Server instance. This vulnerability was fixed in GitHub Enterprise Server versions 3.0.22, 3.1.14, 3.2.6, and 3.3.1. For more information, please see [this post](#) on the GitHub Blog.
- **December 17, 2021 update:** The fixes in place for this release also mitigate [CVE-2021-45046](#), which was published after this release. No additional upgrade for GitHub Enterprise Server is required to mitigate both CVE-2021-44228 and CVE-2021-45046.

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.
- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Enterprise Server 3.3.0

[Download GitHub Enterprise Server 3.3.0](#)

December 07, 2021

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

For upgrade instructions, see "[Upgrading GitHub Enterprise Server](#)."

Note: We are aware of an issue where GitHub Actions may fail to start automatically following the upgrade to GitHub Enterprise Server 3.3. To resolve, connect to the appliance via SSH and run the `ghe-actions-start` command.

Features

Security Manager role

- Organization owners can now grant teams the access to manage security alerts and settings on their repositories. The "security manager" role can be applied to any team and grants the team's members the following access:
 - Read access on all repositories in the organization.
 - Write access on all security alerts in the organization.
 - Access to the organization-level security tab.
 - Write access on security settings at the organization level.
 - Write access on security settings at the repository level.

The security manager role is available as a public beta and subject to change. For more information, see "[Managing security managers in your organization](#)." [Updated 2022-07-29]

Ephemeral self-hosted runners for GitHub Actions & new webhooks for auto-scaling

- GitHub Actions now supports ephemeral (single job) self-hosted runners and a new `workflow_job` webhook to make autoscaling runners easier.

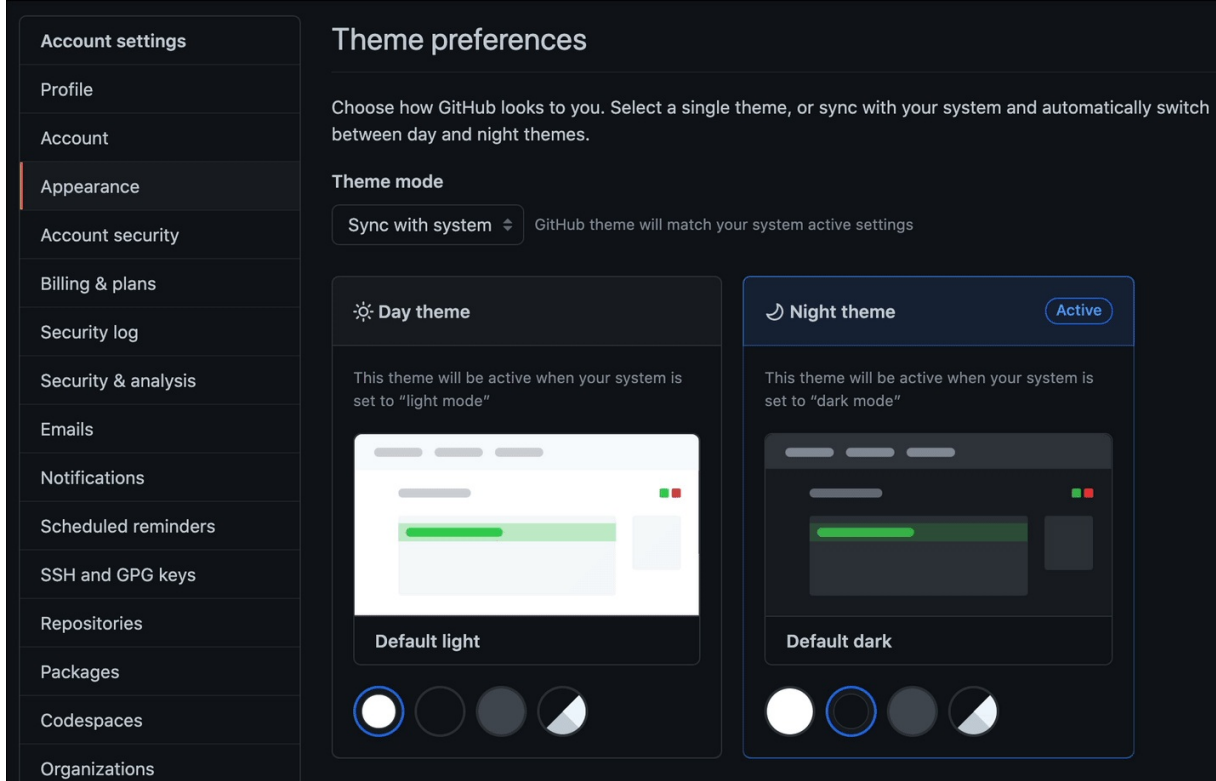
Ephemeral runners are good for self-managed environments where each job is required to run on a clean image. After a job is run, ephemeral runners are automatically unregistered from your GitHub Enterprise Server instance, allowing you to perform any post-job management.

You can combine ephemeral runners with the new `workflow_job` webhook to automatically scale self-hosted runners in response to GitHub Actions job requests.

For more information, see "[Autoscaling with self-hosted runners](#)" and "[Webhook events and payloads](#)."

Dark high contrast theme

- A dark high contrast theme, with greater contrast between foreground and background elements, is now available on GitHub Enterprise Server 3.3. This release also includes improvements to the color system across all GitHub themes.



For more information about changing your theme, see "[Managing your theme settings](#)."

Changes

Administration Changes

- GitHub Enterprise Server 3.3 includes improvements to the maintenance of repositories, especially for repositories that contain many unreachable objects. Note that the first maintenance cycle after upgrading to GitHub Enterprise Server 3.3 may take longer than usual to complete.
- GitHub Enterprise Server 3.3 includes the public beta of a repository cache for geographically-distributed teams and CI infrastructure. The repository cache keeps a read-only copy of your repositories available in additional geographies, which prevents clients from downloading duplicate Git content from your primary instance. For more information, see "[About repository caching](#)."
- GitHub Enterprise Server 3.3 includes improvements to the user impersonation process. An impersonation session now requires a justification for the impersonation, actions are recorded in the audit log as being performed as an impersonated user, and the user who is impersonated will receive an email notification that they have been impersonated by an enterprise administrator. For more information, see "[Impersonating a user](#)."
- A new stream processing service has been added to facilitate the growing set of events that are published to the audit log, including events associated with Git and GitHub Actions activity.
- The GitHub Connect data connection record now includes a list of enabled GitHub Connect features. [Updated 2021-12-09]

Token Changes


- An expiration date can now be set for new and existing personal access tokens. Setting an expiration date on personal access tokens is highly recommended to prevent older tokens from leaking and compromising security. Token owners will receive an email when it's time to renew a token that's about to expire. Tokens that have expired can be regenerated, giving users a duplicate token with the same properties as the original.

When using a personal access token with the GitHub API, a new `GitHub-Authentication-Token-Expiration` header is included in the response, which indicates the token's expiration date. For more information, see "[Creating a personal access token](#)."

Notifications changes

- Notification emails from discussions now include `(Discussion #xx)` in the subject, so you can recognize and filter emails that reference discussions.

Repositories changes

- Public repositories now have a `Public` label next to their names like private and internal repositories. This change makes it easier to identify public repositories and avoid accidentally committing private code.
- If you specify the exact name of a branch when using the branch selector menu, the result now appears at the top of the list of matching branches. Previously, exact branch name matches could appear at the bottom of the list.
- When viewing a branch that has a corresponding open pull request, GitHub Enterprise Server now links directly to the pull request. Previously, there would be a prompt to contribute using branch comparison or to open a new pull request.
- You can now click a button to copy the full raw contents of a file to the clipboard. Previously, you would need to open the raw file, select all, and then copy. To copy the contents of a file, navigate to the file and click  in the toolbar. Note that this feature is currently only available in some browsers.
- When creating a new release, you can now select or create the tag using a dropdown selector, rather than specifying the tag in a text field. For more information, see "[Managing releases in a repository](#)."
- A warning is now displayed when viewing a file that contains bidirectional Unicode text. Bidirectional Unicode text can be interpreted or compiled differently than it appears in a user interface. For example, hidden bidirectional Unicode characters can be used to swap segments of text in a file. For more information about replacing these characters, see the [GitHub changelog](#).
- You can now use `CITATION.cff` files to let others know how you would like them to cite your work. `CITATION.cff` files are plain text files with human- and machine-readable citation information. GitHub Enterprise Server parses this information into common citation formats such as [APA](#) and [BibTeX](#). For more information, see "[About CITATION files](#)."

Markdown changes

- You can use new keyboard shortcuts for quotes and lists in Markdown files, issues, pull requests, and comments.
 - To add quotes, use `cmd shift .` on Mac, or `ctrl shift .` on Windows and Linux.
 - To add an ordered list, use `cmd shift 7` on Mac, or `ctrl shift 7` on Windows and Linux.
 - To add an unordered list, use `cmd shift 8` on Mac, or `ctrl shift 8` on Windows and Linux.

See "[Keyboard shortcuts](#)" for a full list of available shortcuts.

- You can now use footnote syntax in any Markdown field. Footnotes are displayed as superscript links that you can click to jump to the referenced information, which is displayed in a new section at the bottom of the document. For more information about the syntax, see "[Basic writing and formatting syntax](#)."
- When viewing Markdown files, you can now click `<>` in the toolbar to view the source of a Markdown file. Previously, you needed to use the blame view to link to specific line numbers in the source of a Markdown file.
- You can now add images and videos to Markdown files in gists by pasting them into the Markdown body or selecting them from the dialog at the bottom of the Markdown file. For information about supported file types, see "[Attaching files](#)."
- GitHub Enterprise Server now automatically generates a table of contents for Wikis, based on headings.
- When dragging and dropping files into a Markdown editor, such as images and videos, GitHub Enterprise Server

now uses the mouse pointer location instead of the cursor location when placing the file.

Issues and pull requests changes

- You can now search issues by label using a logical OR operator. To filter issues using logical OR, use the comma syntax. For example, `label:"good first issue","bug"` will list all issues with a label of `good first issue` or `bug`. For more information, see "[Filtering and searching issues and pull requests](#)."
- Improvements have been made to help teams manage code review assignments. You can now:
 - Limit assignment to only direct members of the team.
 - Continue with automatic assignment even if one or more members of the team are already requested.
 - Keep a team assigned to review even if one or more members is newly assigned.

The timeline and reviewers sidebar on the pull request page now indicate if a review request was automatically assigned to one or more team members.

For more information, see the [GitHub changelog](#).

- You can now filter pull request searches to only include pull requests you are directly requested to review.
- Filtered files in pull requests are now completely hidden from view, and are no longer shown as collapsed in the "Files Changed" tab. The "File Filter" menu has also been simplified. For more information, see "[Filtering files in a pull request](#)."

GitHub Actions changes

- You can now create "composite actions" which combine multiple workflow steps into one action, and includes the ability to reference other actions. This makes it easier to reduce duplication in workflows. Previously, an action could only use scripts in its YAML definition. For more information, see "[Creating a composite action](#)."
- Managing self-hosted runners at the enterprise level no longer requires using personal access tokens with the `admin:enterprise` scope. You can instead use the new `manage_runners:enterprise` scope to restrict the permissions on your tokens. Tokens with this scope can authenticate to [many REST API endpoints](#) to manage your enterprise's self-hosted runners.
- The audit log now includes additional events for GitHub Actions. Audit log entries are now recorded for the following events:
 - A self-hosted runner is registered or removed.
 - A self-hosted runner is added to a runner group, or removed from a runner group.
 - A runner group is created or removed.
 - A workflow run is created or completed.
 - A workflow job is prepared. Importantly, this log includes the list of secrets that were provided to the runner.

For more information, see "[Security hardening for GitHub Actions](#)."

- GitHub Enterprise Server 3.3 contains performance improvements for job concurrency with GitHub Actions. For more information about the new performance targets for a range of CPU and memory configurations, see "[Getting started with GitHub Actions for GitHub Enterprise Server](#)."
- To mitigate insider man in the middle attacks when using actions resolved through GitHub Connect to GitHub.com from GitHub Enterprise Server, the actions namespace (`owner/name`) is retired on use. Retiring the namespace prevents that namespace from being created on your GitHub Enterprise Server instance, and ensures all workflows referencing the action will download it from GitHub.com.

GitHub Packages changes

- When a repository is deleted, any associated package files are now immediately deleted from your GitHub Packages external storage.

Dependabot and Dependency graph changes

- Dependency review is out of beta and is now generally available for GitHub Advanced Security customers. Dependency review provides an easy-to-understand view of dependency changes and their security impact in the "Files changed" tab of pull requests. It informs you of which dependencies were added, removed, or updated, along with vulnerability information. For more information, see "[Reviewing dependency changes in a pull request](#)."
- Dependabot is now available as a private beta, offering both version updates and security updates for several popular ecosystems. Dependabot on GitHub Enterprise Server requires GitHub Actions and a pool of self-hosted runners configured for Dependabot use. Dependabot on GitHub Enterprise Server also requires GitHub Connect to be enabled. To learn more and sign up for the beta, contact the GitHub Sales team.

Code scanning and secret scanning changes

- The depth of CodeQL's analysis has been improved by adding support for more [libraries and frameworks](#) and increasing the coverage of our existing library and framework models. [JavaScript](#) analysis now supports most common templating languages, and [Java](#) now covers more than three times the endpoints of previous CodeQL versions. As a result, CodeQL can now detect even more potential sources of untrusted user data, steps through which that data flows, and potentially dangerous sinks where the data could end up. This results in an overall improvement of the quality of code scanning alerts.
- CodeQL now supports scanning standard language features in Java 16, such as records and pattern matching. CodeQL is able to analyze code written in Java version 7 through 16. For more information about supported languages and frameworks, see the [CodeQL documentation](#).
- Improvements have been made to the code scanning `on:push` trigger when code is pushed to a pull request. If an `on:push` scan returns results that are associated with a pull request, code scanning will now show these alerts on the pull request.

Some other CI/CD systems can be exclusively configured to trigger a pipeline when code is pushed to a branch, or even exclusively for every commit. Whenever such an analysis pipeline is triggered and results are uploaded to the SARIF API, code scanning will also try to match the analysis results to an open pull request. If an open pull request is found, the results will be published as described above. For more information, see the [GitHub changelog](#).

- You can now use the new pull request filter on the code scanning alerts page to find all the code scanning alerts associated with a pull request. A new "View all branch alerts" link on the pull request "Checks" tab allows you to directly view code scanning alerts with the specific pull request filter already applied. For more information, see the [GitHub changelog](#).
- User defined patterns for secret scanning is out of beta and is now generally available for GitHub Advanced Security customers. Also new in this release is the ability to edit custom patterns defined at the repository, organization, and enterprise levels. After editing and saving a pattern, secret scanning searches for matches both in a repository's entire Git history and in any new commits. Editing a pattern will close alerts previously associated with the pattern if they no longer match the updated version. Other improvements, such as dry-runs, are planned in future releases. For more information, see "[Defining custom patterns for secret scanning](#)."

API and webhook changes

- Most REST API previews have graduated and are now an official part of the API. Preview headers are no longer required for most REST API endpoints, but will still function as expected if you specify a graduated preview in the `Accept` header of a request. For previews that still require specifying the preview in the `Accept` header of a request, see "[API previews](#)."
- You can now use the REST API to configure custom autolinks to external resources. The REST API now provides beta `GET / POST / DELETE` endpoints which you can use to view, add, or delete custom autolinks associated with a repository. For more information, see "[Autolinks](#)."
- You can now use the REST API to sync a forked repository with its upstream repository. For more information, see "[Branches](#)" in the REST API documentation.
- Enterprise administrators on GitHub Enterprise Server can now use the REST API to enable or disable Git LFS for a

repository. For more information, see "[Repositories](#)."

- You can now use the REST API to query the audit log for an enterprise. While audit log forwarding provides the ability to retain and analyze data with your own toolkit and determine patterns over time, the new endpoint can help you perform limited analysis on recent events. For more information, see "[GitHub Enterprise administration](#)" in the REST API documentation.
- GitHub App user-to-server API requests can now read public resources using the REST API. This includes, for example, the ability to list a public repository's issues and pull requests, and to access a public repository's comments and content.
- When creating or updating a repository, you can now configure whether forking is allowed using the REST and GraphQL APIs. Previously, APIs for creating and updating repositories didn't include the fields `allow_forking` (REST) or `forkingAllowed` (GraphQL). For more information, see "[Repositories](#)" in the REST API documentation and "[Repositories](#)" in the GraphQL API documentation.
- A new GraphQL mutation `createCommitOnBranch` makes it easier to add, update, and delete files in a branch of a repository. Compared to the REST API, you do not need to manually create blobs and trees before creating the commit. This allows you to add, update, or delete multiple files in a single API call.

Commits authored using the new API are automatically GPG signed and are [marked as verified](#) in the GitHub Enterprise Server UI. GitHub Apps can use the mutation to author commits directly or [on behalf of users](#).

- When a new tag is created, the [push](#) webhook payload now always includes a `head_commit` object that contains the data of the commit that the new tag points to. As a result, the `head_commit` object will always contain the commit data of the payload's `after` commit.

Performance Changes

- Page loads and jobs are now significantly faster for repositories with many Git refs.

Known issues

- After upgrading to GitHub Enterprise Server 3.3, GitHub Actions may fail to start automatically. To resolve this issue, connect to the appliance via SSH and run the `ghe-actions-start` command.
- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- GitHub Actions storage settings cannot be validated and saved in the Management Console when "Force Path Style" is selected, and must instead be configured with the `ghe-actions-precheck` command line utility.

- GitHub Enterprise Server 3.3 instances installed on Azure and provisioned with 32+ CPU cores would fail to launch, due to a bug present in the current Linux kernel. [Updated: 2022-04-08]
- In some cases, GitHub Advanced Security customers who upgrade to GitHub Enterprise Server 3.5 or later may notice that alerts from secret scanning are missing in the web UI and REST API. To ensure the alerts remain visible, do not skip 3.4 when you upgrade from an earlier release to 3.5 or later. A fix is available in the [3.5.5](#) and [3.6.1](#) patch releases.

To plan an upgrade through 3.4, see the [Upgrade assistant](#). [Updated: 2022-09-01]

Deprecations

Deprecation of GitHub Enterprise Server 2.22

- **GitHub Enterprise Server 2.22 was discontinued on September 23, 2021.** This means that no patch releases will be made, even for critical security issues, after this date. For better performance, improved security, and new features, [upgrade to the newest version of GitHub Enterprise Server](#) as soon as possible.

Deprecation of GitHub Enterprise Server 3.0

- **GitHub Enterprise Server 3.0 will be discontinued on February 16, 2022.** This means that no patch releases will be made, even for critical security issues, after this date. For better performance, improved security, and new features, [upgrade to the newest version of GitHub Enterprise Server](#) as soon as possible.

Deprecation of XenServer Hypervisor support

- Starting with GitHub Enterprise Server 3.3, GitHub Enterprise Server on XenServer is deprecated and is no longer supported. Please contact [GitHub Support](#) with questions or concerns.

Deprecation of OAuth Application API endpoints and API authentication using query parameters

- To prevent accidental logging or exposure of `access_tokens`, we discourage the use of OAuth Application API endpoints and the use of API authentication using query parameters. View the following posts to see the proposed replacements:
 - [Replacement OAuth Application API endpoints](#)
 - [Replacement authentication using headers instead of query param](#)

These endpoints and authentication route are planned to be removed from GitHub Enterprise Server in GitHub Enterprise Server 3.4.

Deprecation of the CodeQL runner

- The CodeQL runner is being deprecated. GitHub Enterprise Server 3.3 will be the final release series that supports the CodeQL runner. Starting with GitHub Enterprise Server 3.4, the CodeQL runner will be removed and no longer supported. The CodeQL CLI version 2.6.2 or greater is a feature-complete replacement for the CodeQL runner. For more information, see the [GitHub changelog](#).

Deprecation of custom bit-cache extensions

- Starting in GitHub Enterprise Server 3.1, support for GitHub's proprietary bit-cache extensions began to be phased out. These extensions are now deprecated in GitHub Enterprise Server 3.3.

Any repositories that were already present and active on your GitHub Enterprise Server instance running version 3.1 or 3.2 will have been automatically updated.

Repositories which were not present and active before upgrading to GitHub Enterprise Server 3.3 may not perform optimally until a repository maintenance task is run and has successfully completed.

To start a repository maintenance task manually, browse to

`https://<hostname>/stafftools/repositories/<owner>/<repository>/network` for each affected repository and click the **Schedule** button.

Change to the format of authentication tokens affects GitHub Connect

- GitHub Connect will no longer work after June 3rd for instances running GitHub Enterprise Server 3.1 or older, due to the format of GitHub authentication tokens changing. To continue using GitHub Connect, upgrade to GitHub Enterprise Server 3.2 or later. For more information, see the [GitHub Blog](#). [Updated: 2022-06-14]

Backups

- GitHub Enterprise Server 3.3 requires at least [GitHub Enterprise Backup Utilities 3.3.0](#) for [Backups and Disaster Recovery](#).