

This version of GitHub Enterprise was discontinued on 2023-03-15. 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 3.4 release notes







Enterprise Server 3.4.18

[Download GitHub Enterprise Server 3.4.18](#)

March 23, 2023

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

3.4.18: Security fixes

- **HIGH:** Addressed an improper authentication vulnerability that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH certificate authority. This vulnerability was reported via the  [GitHub Bug Bounty Program](#)  and has been assigned  [CVE-2023-23761](#). [Updated: 2023-04-07]
- **MEDIUM:** Addressed an incorrect comparison vulnerability that allowed commit smuggling by displaying an incorrect diff. This vulnerability was reported via the  [GitHub Bug Bounty Program](#)  and has been assigned  [CVE-2023-23762](#). [Updated: 2023-04-07]

3.4.18: Bug fixes

- In the Management Console's monitor dashboard, the `Cached Requests` and `Served Requests` graphs, which are retrieved by the `git fetch catching` command, did not display metrics for the instance.
- After a site administrator exempted the `@github-actions[bot]` user from rate limiting by using the `ghe-config app.github.rate-limiting-exempt-users "github-actions[bot]"` command, running `ghe-config-check` caused a `Validation is-valid-character set failed` warning to appear.
- GitHub Actions (`actions`) and Microsoft SQL (`mssql`) did not appear in the list of processes within the instances monitor dashboard.
- On an instance in a high availability configuration, if an administrator tore down replication from a replica node using `ghe-repl-teardown` immediately after running `ghe-repl-setup`, but before `ghe-repl-start`, an error indicated that the script `cannot launch /usr/local/bin/ghe-single-config-apply - run is locked`. `ghe-repl-teardown` now displays an informational alert and continues the teardown.
- On an instance in a cluster configuration, when a site administrator set maintenance mode using `ghe-maintenance -s`, a `Permission denied` error appeared when the utility tried to access `/data/user/common/cluster.conf`.
- When a site administrator used `ghe-migrator` to migrate data to GitHub Enterprise Server, in some cases, nested team relationships would not persist after teams were imported.

- GitHub Enterprise Server published distribution metrics that cannot be processed by collectd. The metrics included `pre_receive.lfsintegrity.dist.referenced_oids`, `pre_receive.lfsintegrity.dist.unknown_oids`, and `git.hooks.runtime`.
-

3.4.18: Changes

- After an enterprise owner enables Dependabot updates, the instance creates the initial set of updates faster.
 - On an instance in a cluster configuration, when a site administrator sets maintenance mode on a single cluster node using `ghe-maintenance -s`, the utility warns the administrator to use `ghe-cluster-maintenance -s` to set maintenance mode on all of the clusters nodes. For more information, see "[Enabling and scheduling maintenance mode](#)."
 - When a site administrator configures an outbound web proxy server for GitHub Enterprise Server, the instance now validates top-level domains (TLDs) excluded from the proxy configuration. By default, you can exclude public TLDs that the IANA specifies. Site administrators can specify a list of unregistered TLDs to exclude using `ghe-config`. The `.` prefix is required for any public TLDs. For example, `.example.com` is valid, but `example.com` is invalid. For more information, see "[Configuring an outbound web proxy server](#)."
 - The default path for output from `ghe-saml-mapping-csv -d` is `/data/user/tmp` instead of `/tmp`. For more information, see "[Command-line utilities](#)."
-

3.4.18: Known issues

- 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.
- 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.
- Hotpatch upgrades to GitHub Enterprise Server 3.4.9 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]

- 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]

- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.

Enterprise Server 3.4.17

[Download GitHub Enterprise Server 3.4.17](#)

March 02, 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.

3.4.17: 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 GitHub Enterprise Server instance. This vulnerability was reported via the [GitHub Bug Bounty Program](#) and has been assigned [CVE-2023-23760](#). [Updated: 2023-03-10]

3.4.17: Bug fixes

- When viewing a list of open sessions for the devices logged into a user account, the GitHub Enterprise Server web UI could display an incorrect location.
- In the rare case when primary shards for Elasticsearch were located on a replica node, the `ghe-repl-stop` command would fail with `ERROR: Running migrations`.

3.4.17: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.9 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 3.4.16

[Download GitHub Enterprise Server 3.4.16](#)

February 16, 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.

3.4.16: Security fixes [↗](#)

- **HIGH:** Updated Git to include fixes from 2.39.2, which address [CVE-2023-22490](#) and [CVE-2023-23946](#).
- Packages have been updated to the latest security versions.

3.4.16: Known issues [↗](#)

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.9 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 3.4.15

February 02, 2023

[Download GitHub Enterprise Server 3.4.15](#)

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

3.4.15: Security fixes

- **MEDIUM:** A code injection vulnerability was identified in GitHub Enterprise Server that allowed setting arbitrary

environment variables from a single environment variable value in GitHub Actions when using a Windows based runner due to improper sanitization of null bytes. To exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability was reported via the [GitHub Bug Bounty Program](#) and has been assigned [CVE-2023-22381](#).

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

3.4.15: Bug fixes [↗](#)

- During the validation phase of a configuration run, a `No such object error` may have occurred for the Notebook and Viewscreen services.
 - When enabling automatic TLS certificate management with Let's Encrypt, the process could fail with the error `The certificate is not signed by a trusted certificate authority (CA) or the certificate chain is missing intermediate CA signing certificates`.
-

3.4.15: Changes [↗](#)

- When a timeout occurs during diff generation, such as when a commit displays an error that the diff is taking too long to generate, the `push` webhook event will deliver empty diff information. Previously, the `push` webhook event would fail to be delivered.
-

3.4.15: Known issues [↗](#)

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.14

[Download GitHub Enterprise Server 3.4.14](#)

January 17, 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.

3.4.14: Security fixes

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

3.4.14: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.13

[Download GitHub Enterprise Server 3.4.13](#)

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.

3.4.13: Security fixes [↗](#)

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

3.4.13: 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.
 - Repositories locked for migration would allow files to be edited in the web UI.
 - The `git-janitor` command was unable to fix outdated `multi-pack-index.lock` files, resulting in the repository failing maintenance.
-

3.4.13: Changes [↗](#)

- The `ghe-support-bundle` and `ghe-cluster-support-bundle` commands were updated to include the `-p/--period` flag to generate a time constrained support bundle. The duration can be specified in days and hours, for example: `-p '2 hours'`, `-p '1 day'`, `-p '2 days 5 hours'`.
- 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.

3.4.13: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.12

[Download GitHub Enterprise Server 3.4.12](#)

December 13, 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.

3.4.12: 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](#).
 - **MEDIUM:** An information disclosure vulnerability was identified in GitHub Enterprise Server that allowed private repositories to be added to a GitHub Actions runner group via the API by a user who did not have access to those repositories, resulting in the repository names being shown in the UI. To exploit this vulnerability, an attacker would need access to the GHES instance, permissions to modify GitHub Actions runner groups, and successfully guess the obfuscated ID of private repositories. This vulnerability was reported via the [GitHub Bug Bounty Program](#) and has been assigned [CVE-2022-46257](#).
-

3.4.12: Bug fixes

- When a site administrator ran the `ghe-repl-sync-ca-certificates` command from an instances primary node via the administrative shell (SSH), the command only replicated CA certificates from the instances primary node to a single replica node. The command did not replicate the certificates to all available replica nodes.
 - 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.
 - The `member` webhook event did not include the `from` and `to` field values for the `permission` field as part of the `changes` field.
 - After a user's account was deleted from the instance, image attachments that the user uploaded in comments were no longer visible in the web interface.
 - A debug-level message appeared in a system log, which could consume space rapidly on the instance's root storage volume.
-

3.4.12: Known issues

- 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.
- 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.

- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.11

[Download GitHub Enterprise Server 3.4.11](#)

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.

3.4.11: 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 "[Repository contents](#)" should enforce workflow scope. This vulnerability was reported via the [GitHub Bug Bounty program](#) and has been assigned [CVE-2022-46258](#).

3.4.11: Bug fixes

- If GitHub Actions was configured with S3 blob storage for the instance, content like logs and artifacts from deleted or expired workflow runs would remain in blob storage indefinitely. The instance will delete this content automatically the next time a regular background cleanup job runs.
- Setting the maintenance mode with an IP Exception List would not persist across upgrades.

- GitHub Pages builds could time out on instances in AWS that are configured for high availability.
 - 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.
 - In some cases, users could not merge a pull request due to unexpected status checks.
 - After running migrations for the GitHub Enterprise Importer on an instance configured for high availability, replication of migration storage assets would not catch up.
 - Zombie processes no longer accumulate in the `gitrpcd` container.
-

3.4.11: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

3.4.10: 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 Redis to 5.0.14 to address [CVE-2021-32672](#) and [CVE-2021-32762](#).
- **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:** 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.

3.4.10: 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.
- When a user accessed a renamed repository using Git, the hostname in the Git output incorrectly indicated GitHub.com instead of the instance's hostname.
- 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.

3.4.10: 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](#)."

3.4.10: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.9

September 21, 2022

[Download GitHub Enterprise Server 3.4.9](#)

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

3.4.9: Features

- Repository archives for migrations now include an `is_archived` field.
-

3.4.9: 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.
 - **LOW:** Granting a user the ability to bypass branch protections no longer allows the user to bypass the requirement for signature verification.
 - Packages have been updated to the latest security versions.
-

3.4.9: 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.
- The `ghe-find-insecure-git-operations` command did not return all insecure Git operations after each invocation.
- In rare cases, an upgrade from GitHub Enterprise Server 3.3 to 3.4 would incorrectly modify how data is stored, resulting in failures during future upgrades. When upgrading directly to this release from 3.3, the failure will not occur.
- 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.
- After upgrading to GitHub Enterprise Server 3.4, releases would appear to be missing from repositories. This occurred when the required Elasticsearch index migrations had not successfully completed. The releases UI now indicates if it is waiting for the Elasticsearch index migrations to complete, and links to documentation on how to observe status and immediately complete the migration.
- 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.
- If branch protections were enabled, the `GITHUB_REF_PROTECTED` environment variable and `github.ref_protected` contexts for GitHub Actions workflow runs were incorrectly set as `false`.
- When using a VPC endpoint URL as an AWS S3 URL for GitHub Packages, publication and installation of packages failed.

- When adding a member to an organization, an erroneous SAML SSO trial invitation appeared.

3.4.9: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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 3.4.9 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

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

3.4.8: 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.
 - The site admin page for individual users at `http(s)://HOSTNAME/stafftools/users/USERNAME/admin` contained functionality not intended for GitHub Enterprise Server.
 - 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.
-

3.4.8: 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](#)."
 - APIs that contain the `organization` or `org` route now accept either the organization's slug or ID. Previously, the APIs only accepted slugs, which caused `Link` headers for GitHub Advanced Security endpoints to be inaccessible. For more information, see "[Organizations](#)" in the REST API documentation.
 - 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](#)."
-

3.4.8: Known issues

- 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.

- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

Enterprise Server 3.4.7

[Download GitHub Enterprise Server 3.4.7](#)

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.

3.4.7: 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](#).

3.4.7: Bug fixes

- In some cases, GitHub Enterprise Server instances on AWS that used the `r4.4xlarge` instance type would fail to boot.
 - When calculating committers for GitHub Advanced Security, it was not possible to specify individual repositories. For more information, see "[Site admin dashboard](#)."
 - 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](#)."
-

3.4.7: Changes [↗](#)

- `pre_receive_hook.rejected_push` events were not displayed in the enterprise audit log.
 - Both migration archives for repositories and archive exports for user accounts include release reactions.
-

3.4.7: Known issues [↗](#)

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]
-

Enterprise Server 3.4.6

[Download GitHub Enterprise Server 3.4.6](#)

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.

3.4.6: 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](#).
-

3.4.6: Bug fixes

- 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.
 - In some cases, scheduled GitHub Actions workflows could become disabled.
 - The Billing API's "[Billing](#)" endpoint now returns `Link` headers to provide information about pagination.
 - The Billing API's "[Billing](#)" endpoint now returns the correct number of total committers.
-

3.4.6: 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.
-

3.4.6: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

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

3.4.5: Security fixes [↗](#)

- **MEDIUM:** Prevents an attack where an `org` query string parameter can be specified for a GitHub Enterprise Server URL that then gives access to another organization's active committers.
 - **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.
-

3.4.5: Bug fixes [↗](#)

- Files inside an artifact archive were unable to be opened after decompression due to restrictive permissions.
 - Redis timeouts no longer halt database migrations while running `ghe-config-apply`.
 - Background job processors would get stuck in a partially shut-down state, resulting in certain kinds of background jobs (like code scanning) appearing stuck.
 - In some cases, site administrators were not automatically added as enterprise owners.
 - A rendering issue could affect the dropdown list for filtering secret scanning alerts in a repository.
-

3.4.5: Changes [↗](#)

- Improved the performance of Dependabot version updates after first enabled.
 - The GitHub Pages build and synchronization timeouts are now configurable in the Management Console.
 - 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.
 - When [deploying cache-server nodes](#), it is now mandatory to describe the datacenter topology (using the `--datacenter` argument) for every node in the system. This requirement prevents situations where leaving datacenter membership set to "default" leads to workloads being inappropriately balanced across multiple datacenters.
-

3.4.5: Known issues [↗](#)

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration.
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

Enterprise Server 3.4.4

[Download GitHub Enterprise Server 3.4.4](#)

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.

3.4.4: Security fixes

- Packages have been updated to the latest security versions.

3.4.4: 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.
 - When GitHub Actions was enabled but TLS was disabled on GitHub Enterprise Server 3.4.1 and later, applying a configuration update would fail.
 - 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.
 - The [GitHub Advanced Security billing API](#) endpoints were not enabled and accessible.
 - Image attachments that were deleted would return a `500 Internal Server Error` instead of a `404 Not Found` error.
 - In environments configured with a repository cache server, the `ghe-repl-status` command incorrectly showed gists as being under-replicated.
 - The "Get a commit" and "Compare two commits" endpoints in the [Commit API](#) would return a `500` error if a file path in the diff contained an encoded and escaped unicode character.
 - 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.
 - The activity timeline for secret scanning alerts wasn't displayed.
-

3.4.4: 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.
-

3.4.4: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both

enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]

- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

Enterprise Server 3.4.3

[Download GitHub Enterprise Server 3.4.3](#)

May 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.

3.4.3: 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.

3.4.3: 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.
- When adding custom patterns and providing non-UTF8 test strings, match highlighting was incorrect.
- LDAP users with an underscore character (`_`) in their user names can now login successfully.
- 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.

- After enabling SAML encrypted assertions with Azure as identity provider, the sign in page would fail with a 500 error.
 - Character key shortcut preferences weren't respected.
 - 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 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]
 - Upgrades would sometimes fail while migrating dependency graph data. [Updated: 2022-06-30]
-

3.4.3: 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.
 - The Nomad allocation timeout for Dependency Graph has been increased to ensure post-upgrade migrations can complete.
 - 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.
-

3.4.3: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4 releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

Enterprise Server 3.4.2

[Download GitHub Enterprise Server 3.4.2](#)

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.

3.4.2: Security fixes

- Packages have been updated to the latest security versions.

3.4.2: Bug fixes

- 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.
- When a manifest file was deleted from a repository, the manifest would not be removed from the repository's "Dependency graph" page.
- 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.
 - Repository cache servers could serve data from non-cache locations even when the data was available in the local cache location.
 - 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.
 - The `/stafftools/users/ip_addresses/:address` page responded with a `500 Internal Server Error` when attempting to display the page for an IPv6 address.
 - 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.
-

3.4.2: Changes [↗](#)

- Added support for replica domain names that are more than 63 characters.
 - Configuration errors that halt a config apply run are now output to the terminal in addition to the configuration log.
 - If GitHub Advanced Security features are enabled on your instance, the performance of background jobs has improved when processing batches for repository contributions.
-

3.4.2: Known issues [↗](#)

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- After upgrading to GitHub Enterprise Server 3.4, releases may appear to be missing from repositories. This can occur when the required Elasticsearch index migrations have not successfully completed.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]
-

3.4.2: Deprecations

Deprecation of GitHub Enterprise Server 3.0

- **GitHub Enterprise Server 3.0 was 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 GitHub Enterprise Server 3.1

- **GitHub Enterprise Server 3.1 will be discontinued on June 3, 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 in GitHub Enterprise Server 3.3, GitHub Enterprise Server on XenServer was deprecated and is no longer supported. Please contact [GitHub Support](#) with questions or concerns.

Deprecation of the Content Attachments API preview

- Due to low usage, we have deprecated the Content References API preview in GitHub Enterprise Server 3.4. The API was previously accessible with the `corsair-preview` header. Users can continue to navigate to external URLs without this API. Any registered usages of the Content References API will no longer receive a webhook notification for URLs from your registered domain(s) and we no longer return valid response codes for attempted updates to existing content attachments.

Deprecation of the Codes of Conduct API preview

- The Codes of Conduct API preview, which was accessible with the `scarlet-witch-preview` header, is deprecated and no longer accessible in GitHub Enterprise Server 3.4. We instead recommend using the "[Get community profile metrics](#)" endpoint to retrieve information about a repository's code of conduct. For more information, see the "[Deprecation Notice: Codes of Conduct API preview](#)" in the GitHub changelog.

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

- Starting with GitHub Enterprise Server 3.4, the [deprecated version of the OAuth Application API endpoints](#) have been removed. If you encounter 404 error messages on these endpoints, convert your code to the versions of the OAuth Application API that do not have `access_tokens` in the URL. We've also disabled the use of API authentication using query parameters. We instead recommend using [API authentication in the request header](#).

Deprecation of the CodeQL runner

- The CodeQL runner is deprecated in GitHub Enterprise Server 3.4 and is no longer supported. The deprecation only affects users who use CodeQL code scanning in third party CI/CD systems; GitHub Actions users are not affected. We strongly recommend that customers migrate to the CodeQL CLI, which 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 deprecated in GitHub Enterprise Server 3.3 onwards.

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.

Theme picker for GitHub Pages has been removed

- The theme picker for GitHub Pages has been removed from the Pages settings. For more information about configuration of themes for GitHub Pages, see "[Adding a theme to your GitHub Pages site using Jekyll](#)."

3.4.2: Backups

- GitHub Enterprise Server 3.4 requires at least [GitHub Enterprise Backup Utilities 3.4.0](#) for [Backups and Disaster Recovery](#).

Enterprise Server 3.4.1

[Download GitHub Enterprise Server 3.4.1](#)

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.

3.4.1: 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.
-

3.4.1: Bug fixes

- A workflow run may not complete if it uses composite-actions.
 - 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.
 - Pre-receive hooks that used `gpg --import` timed out due to insufficient `syscall` privileges.
 - In some cluster topologies, webhook delivery information was not available.
 - The GitHub Actions deployment graph would display an error when rendering a pending job.
 - Elasticsearch health checks would not allow a yellow cluster status when running migrations.
 - When using the [Migrations API](#), queued export jobs were not processed.
 - 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.
 - LDAP user sync jobs would fail when trying to sync GPG keys that had been synced previously.
 - Links to inaccessible pages were removed.
 - Some instances experienced high CPU usage due to large amounts unnecessary background jobs being queued.
 - Empty repositories didnt sync correctly to cache servers.
 - 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.
 - Using `ghe-migrator` or exporting from GitHub.com, an export would not include pull request attachments.
-

3.4.1: 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.
 - The [Migrations API](#) now generates exports of repositories.
 - 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.
-

3.4.1: Known issues

- 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.
- 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.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- When using SAML encrypted assertions with GitHub Enterprise Server 3.4.0 and 3.4.1, a new XML attribute `WantAssertionsEncrypted` in the `SPSSODescriptor` contains an invalid attribute for SAML metadata. IdPs that consume this SAML metadata endpoint may encounter errors when validating the SAML metadata XML schema. A fix will be available in the next patch release. [Updated: 2022-04-11]

To work around this problem, you can take one of the two following actions.

- Reconfigure the IdP by uploading a static copy of the SAML metadata without the `WantAssertionsEncrypted` attribute.
- Copy the SAML metadata, remove `WantAssertionsEncrypted` attribute, host it on a web server, and reconfigure the IdP to point to that URL.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]

3.4.1: Deprecations

Deprecation of GitHub Enterprise Server 3.0

- **GitHub Enterprise Server 3.0 was 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 GitHub Enterprise Server 3.1

- **GitHub Enterprise Server 3.1 will be discontinued on June 3, 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 in GitHub Enterprise Server 3.3, GitHub Enterprise Server on XenServer was deprecated and is no longer supported. Please contact [GitHub Support](#) with questions or concerns.

Deprecation of the Content Attachments API preview

- Due to low usage, we have deprecated the Content References API preview in GitHub Enterprise Server 3.4. The API was previously accessible with the `corsair-preview` header. Users can continue to navigate to external URLs without this API. Any registered usages of the Content References API will no longer receive a webhook notification for URLs from your registered domain(s) and we no longer return valid response codes for attempted updates to existing content attachments.

Deprecation of the Codes of Conduct API preview

- The Codes of Conduct API preview, which was accessible with the `scarlet-witch-preview` header, is deprecated and no longer accessible in GitHub Enterprise Server 3.4. We instead recommend using the "[Get community profile metrics](#)" endpoint to retrieve information about a repository's code of conduct. For more information, see the "[Deprecation Notice: Codes of Conduct API preview](#)" in the GitHub changelog.

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

- Starting with GitHub Enterprise Server 3.4, the [deprecated version of the OAuth Application API endpoints](#) have been removed. If you encounter 404 error messages on these endpoints, convert your code to the versions of the OAuth Application API that do not have `access_tokens` in the URL. We've also disabled the use of API authentication using query parameters. We instead recommend using [API authentication in the request header](#).

Deprecation of the CodeQL runner

- The CodeQL runner is deprecated in GitHub Enterprise Server 3.4 and is no longer supported. The deprecation only affects users who use CodeQL code scanning in third party CI/CD systems; GitHub Actions users are not affected. We strongly recommend that customers migrate to the CodeQL CLI, which 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 deprecated in GitHub Enterprise Server 3.3 onwards.

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.

3.4.1: Backups

- GitHub Enterprise Server 3.4 requires at least [GitHub Enterprise Backup Utilities 3.4.0](#) for [Backups and Disaster Recovery](#).

Enterprise Server 3.4.0

[Download GitHub Enterprise Server 3.4.0](#)

March 15, 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.

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

This release is dedicated to our colleague and friend John, a Hubber who was always there to help. You will be greatly missed.

John "Ralph" Wiebalk 1986-2021

3.4.0: Features

Secret scanning REST API now returns locations

- GitHub Advanced Security customers can now use the REST API to retrieve commit details of secrets detected in private repository scans. The new endpoint returns details of a secret's first detection within a file, including the secret's location and commit SHA. For more information, see "[Secret scanning](#)" in the REST API documentation.

Export license data of committer-based billing for GitHub Advanced Security

- Enterprise and organization owners can now export their GitHub Advanced Security license usage data to a CSV file. The Advanced Security billing data can also be retrieved via billing endpoints in the REST API. For more information, see the "[GitHub changelog](#)."

GitHub Actions reusable workflows in public beta

- You can now reuse entire workflows as if they were an action. This feature is available in public beta. Instead of copying and pasting workflow definitions across repositories, you can now reference an existing workflow with a single line of configuration. For more information, see the "[GitHub changelog](#)."

Dependabot security and version updates in public beta

- Dependabot is now available in GitHub Enterprise Server 3.4 as a public 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 and Dependabot to be enabled by an administrator. Beta feedback and suggestions can be shared in the [Dependabot Feedback GitHub discussion](#). For more information and to try the beta, see "[Setting up Dependabot security and version updates on your enterprise](#)."

SAML authentication supports encrypted assertions

- If you use SAML authentication for GitHub Enterprise Server, you can now configure encrypted assertions from your IdP to improve security. Encrypted assertions add an additional layer of encryption when your IdP transmits information to your GitHub Enterprise Server instance. For more information, see "[Using SAML](#)."

Edit files within pull requests in GitHub Mobile for iOS

- In GitHub Mobile for iOS 1.80.0 and later, users can now edit files within a pull request's topic branch. Support for editing files will come to GitHub Mobile for Android in a future release. [Updated: 2022-09-13]

3.4.0: Changes

Administration Changes

- Users can now choose the number of spaces a tab is equal to, by setting their preferred tab size in the "Appearance" settings of their user account. All code with a tab indent will render using the preferred tab size.
- The GitHub Connect data connection record now includes a count of the number of active and dormant users and the configured dormancy period.
- You can now give users access to enterprise-specific links by adding custom footers to GitHub Enterprise Server. For more information, see "[Configuring custom footers](#)."

Performance Changes

- WireGuard, used to secure communication between GitHub Enterprise Server instances in a High Availability configuration, has been migrated to the Kernel implementation.

Notification Changes

- Organization owners can now unsubscribe from email notifications when new deploy keys are added to repositories belonging to their organizations. For more information, see "[Configuring notifications](#)."
- Notification emails from newly created issues and pull requests now include `(Issue #xx)` or `(PR #xx)` in the email subject, so you can recognize and filter emails that reference these types of issues.

Organization Changes

- Organizations can now display a `README.md` file on their profile Overview. For more information, see the "[GitHub changelog](#)."

- Members of organizations can now view a list of their enterprise owners under the organization's "People" tab. The enterprise owners list is also now accessible using the GraphQL API. For more information, see the "[enterpriseOwners](#)" field under the Organization object in the GraphQL API documentation.

Repositories changes

- A "Manage Access" section is now shown on the "Collaborators and teams" page in your repository settings. The new section makes it easier for repository administrators to see and manage who has access to their repository, and the level of access granted to each user. Administrators can now:
 - Search all members, teams and collaborators who have access to the repository.
 - View when members have mixed role assignments, granted to them directly as individuals or indirectly via a team. This is visualized through a new "mixed roles" warning, which displays the highest level role the user is granted if their permission level is higher than their assigned role.
 - Manage access to popular repositories reliably, with page pagination and fewer timeouts when large groups of users have access.
- GitHub Enterprise Server 3.4 includes improvements to the repository invitation experience, such as notifications for private repository invites, a UI prompt when visiting a private repository you have a pending invitation for, and a banner on a public repository overview page when there is an pending invitation.
- You can now use single-character prefixes for custom autolinks. Autolink prefixes also now allow `.`, `-`, `_`, `+`, `=`, `:`, `/`, and `#` characters, as well as alphanumerics. For more information about custom autolinks, see "[Configuring autolinks to reference external resources](#)."
- A `CODE_OF_CONDUCT.md` file in the root of a repository is now highlighted in the "About" sidebar on the repository overview page.

Releases changes

- GitHub Enterprise Server 3.4 includes improvements to the Releases UI, such as automatically generated release notes which display a summary of all the pull requests for a given release. For more information, see the "[GitHub changelog](#)."
- When a release is published, an avatar list is now displayed at the bottom of the release. Avatars for all user accounts mentioned in the release notes are shown. For more information, see "[Managing releases in a repository](#)."

Markdown changes

- You can now use the new "Accessibility" settings page to manage your keyboard shortcuts. You can choose to disable keyboard shortcuts that only use single characters like `s`, `g`, `c`, and `.` (the period key). For more information, see the "[GitHub changelog](#)."
- You can now choose to use a fixed-width font in Markdown-enabled fields, like issue comments and pull request descriptions. For more information, see the "[GitHub changelog](#)."
- You can now paste a URL on selected text to quickly create a Markdown link. This works in all Markdown-enabled fields, such as issue comments and pull request descriptions. For more information, see the "[GitHub changelog](#)."
- An image URL can now be appended with a theme context, such as `#gh-dark-mode-only`, to define how the Markdown image is displayed to a viewer. For more information, see the "[GitHub changelog](#)."
- When creating or editing a gist file with the Markdown (`.md`) file extension, you can now use the "Preview" or "Preview Changes" tab to display a Markdown rendering of the file contents. For more information, see the "[GitHub changelog](#)."
- When typing the name of a GitHub user in issues, pull requests and discussions, the @mention suggester now ranks existing participants higher than other GitHub users, so that it's more likely the user you're looking for will be listed.
- Right-to-left languages are now supported natively in Markdown files, issues, pull requests, discussions, and comments.

Issues and pull requests changes

- The diff setting to hide whitespace changes in the pull request "Files changed" tab is now retained for your user account for that pull request. The setting you have chosen is automatically reapplied if you navigate away from the page and then revisit the "Files changed" tab of the same pull request.
- When using auto assignment for pull request code reviews, you can now choose to only notify requested team members independently of your auto assignment settings. This setting is useful in scenarios where many users are auto assigned but not all users require notification. For more information, see the "[GitHub changelog](#)."

Branches changes

- Organization and repository administrators can now trigger webhooks to listen for changes to branch protection rules on their repositories. For more information, see the "[branch_protection_rule](#)" event in the webhooks events and payloads documentation.
- When configuring protected branches, you can now enforce that a required status check is provided by a specific GitHub App. If a status is then provided by a different application, or by a user via a commit status, merging is prevented. This ensures all changes are validated by the intended application. For more information, see the "[GitHub changelog](#)."
- Only users with administrator permissions are now able to rename protected branches and modify branch protection rules. Previously, with the exception of the default branch, a collaborator could rename a branch and consequently any non-wildcard branch protection rules that applied to that branch were also renamed. For more information, see "[Renaming a branch](#)" and "[Managing a branch protection rule](#)."
- Administrators can now allow only specific users and teams to bypass pull request requirements. For more information, see the "[GitHub changelog](#)."
- Administrators can now allow only specific users and teams to force push to a repository. For more information, see the "[GitHub changelog](#)."
- When requiring pull requests for all changes to a protected branch, administrators can now choose if approved reviews are also a requirement. For more information, see the "[GitHub changelog](#)."

GitHub Actions changes

- GitHub Actions workflows triggered by Dependabot for the `create`, `deployment`, and `deployment_status` events now always receive a read-only token and no secrets. Similarly, workflows triggered by Dependabot for the `pull_request_target` event on pull requests where the base ref was created by Dependabot, now always receive a read-only token and no secrets. These changes are designed to prevent potentially malicious code from executing in a privileged workflow. For more information, see "[Automating Dependabot with GitHub Actions](#)."
- Workflow runs on `push` and `pull_request` events triggered by Dependabot will now respect the permissions specified in your workflows, allowing you to control how you manage automatic dependency updates. The default token permissions will remain read-only. For more information, see the "[GitHub changelog](#)."
- GitHub Actions workflows triggered by Dependabot will now be sent the Dependabot secrets. You can now pull from private package registries in your CI using the same secrets you have configured for Dependabot to use, improving how GitHub Actions and Dependabot work together. For more information, see "[Automating Dependabot with GitHub Actions](#)."
- You can now manage runner groups and see the status of your self-hosted runners using new Runners and Runner Groups pages in the UI. The Actions settings page for your repository or organization now shows a summary view of your runners, and allows you to deep dive into a specific runner to edit it or see what job it may be currently running. For more information, see the "[GitHub changelog](#)."
- Actions authors can now have their action run in Node.js 16 by specifying `runs.using as node16` in the action's `action.yml`. This is in addition to the existing Node.js 12 support; actions can continue to specify `runs.using: node12` to use the Node.js 12 runtime.
- For manually triggered workflows, GitHub Actions now supports the `choice`, `boolean`, and `environment` input types

in addition to the default `string` type. For more information, see "[on.workflow_dispatch.inputs](#)."

- Actions written in YAML, also known as composite actions, now support `if` conditionals. This lets you prevent specific steps from executing unless a condition has been met. Like steps defined in workflows, you can use any supported context and expression to create a conditional.
- The search order behavior for self-hosted runners has now changed, so that the first available matching runner at any level will run the job in all cases. This allows jobs to be sent to self-hosted runners much faster, especially for organizations and enterprises with lots of self-hosted runners. Previously, when running a job that required a self-hosted runner, GitHub Actions would look for self-hosted runners in the repository, organization, and enterprise, in that order.
- Runner labels for GitHub Actions self-hosted runners can now be listed, added and removed using the REST API. For more information about using the new APIs at a repository, organization, or enterprise level, see "[Repositories](#)", "[Organizations](#)", and "[Enterprises](#)" in the REST API documentation.

Dependabot and Dependency graph changes

- Dependency graph now supports detecting Python dependencies in repositories that use the Poetry package manager. Dependencies will be detected from both `pyproject.toml` and `poetry.lock` manifest files.
- When configuring Dependabot security and version updates on GitHub Enterprise Server, we recommend you also enable Dependabot in GitHub Connect. This will allow Dependabot to retrieve an updated list of dependencies and vulnerabilities from GitHub.com, by querying for information such as the changelogs of the public releases of open source code that you depend upon. For more information, see "[Enabling the dependency graph and Dependabot alerts for your enterprise](#)."
- Dependabot alerts can now be dismissed using the GraphQL API. For more information, see the "[dismissRepositoryVulnerabilityAlert](#)" mutation in the GraphQL API documentation.

Code scanning and secret scanning changes

- The CodeQL CLI now supports including markdown-rendered query help in SARIF files, so that the help text can be viewed in the code scanning UI when the query generates an alert. For more information, see the "[GitHub changelog](#)."
- The CodeQL CLI and Visual Studio Code extension now support building databases and analyzing code on machines powered by Apple Silicon, such as Apple M1. For more information, see the "[GitHub changelog](#)."
- The depth of CodeQL's analysis has been improved by adding support for more [libraries and frameworks](#) from the Python ecosystem. 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. For more information, see the "[GitHub changelog](#)."
- Code scanning with CodeQL now includes beta support for analyzing code in all common Ruby versions, up to and including 3.02. For more information, see the "[GitHub changelog](#)."
- Several improvements have been made to the code scanning API:
 - The `fixed_at` timestamp has been added to alerts. This timestamp is the first time that the alert was not detected in an analysis.
 - Alert results can now be sorted using `sort` and `direction` on either `created`, `updated` or `number`. For more information, see "[List code scanning alerts for a repository](#)."
 - A `Last-Modified` header has been added to the alerts and alert endpoint response. For more information, see "[Last-Modified](#)" in the Mozilla documentation.
 - The `relatedLocations` field has been added to the SARIF response when you request a code scanning analysis. The field may contain locations which are not the primary location of the alert. See an example in the [SARIF spec](#) and for more information see "[Get a code scanning analysis for a repository](#)."
 - Both `help` and `tags` data have been added to the webhook response alert rule object. For more information, see "[Code scanning alert webhooks events and payloads](#)."
 - Personal access tokens with the `public_repo` scope now have write access for code scanning endpoints on

public repos, if the user has permission.

For more information, see "[Code scanning](#)" in the REST API documentation.

- GitHub Advanced Security customers can now use the REST API to retrieve private repository secret scanning results at the enterprise level. The new endpoint supplements the existing repository-level and organization-level endpoints. For more information, see "[Secret scanning](#)" in the REST API documentation.

Mobile changes

- Support for GitHub Mobile is now enabled by default for new GitHub Enterprise Server instances. If you have not explicitly disabled or enabled GitHub Mobile, GitHub Mobile will be enabled when you upgrade to GitHub Enterprise Server 3.4.0 or later. If you previously disabled or enabled GitHub Mobile for your instance, your preference will be preserved upon upgrade. For more information, see "[Managing GitHub Mobile for your enterprise](#)."

3.4.0: Known issues

- 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.
- 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.
- Actions services needs to be restarted after restoring appliance from backup taken on a different host.
- After registering a self-hosted runner with the `--ephemeral` parameter on more than one level (for example, both enterprise and organization), the runner may get stuck in an idle state and require re-registration. [Updated: 2022-06-17]
- When using SAML encrypted assertions with GitHub Enterprise Server 3.4.0 and 3.4.1, a new XML attribute `WantAssertionsEncrypted` in the `SPSSODescriptor` contains an invalid attribute for SAML metadata. IdPs that consume this SAML metadata endpoint may encounter errors when validating the SAML metadata XML schema. A fix will be available in the next patch release. [Updated: 2022-04-11]

To work around this problem, you can take one of the two following actions.

- Reconfigure the IdP by uploading a static copy of the SAML metadata without the `WantAssertionsEncrypted` attribute.
- Copy the SAML metadata, remove `WantAssertionsEncrypted` attribute, host it on a web server, and reconfigure the IdP to point to that URL.
- 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]

- GitHub Pages builds may time out on instances in AWS that are configured for high availability. [Updated: 2022-11-28]
-

3.4.0: Deprecations

Deprecation of GitHub Enterprise Server 3.0

- **GitHub Enterprise Server 3.0 was 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 GitHub Enterprise Server 3.1

- **GitHub Enterprise Server 3.1 will be discontinued on June 3, 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 in GitHub Enterprise Server 3.3, GitHub Enterprise Server on XenServer was deprecated and is no longer supported. Please contact [GitHub Support](#) with questions or concerns.

Deprecation of the Content Attachments API preview

- Due to low usage, we have deprecated the Content References API preview in GitHub Enterprise Server 3.4. The API was previously accessible with the `corsair-preview` header. Users can continue to navigate to external URLs without this API. Any registered usages of the Content References API will no longer receive a webhook notification for URLs from your registered domain(s) and we no longer return valid response codes for attempted updates to existing content attachments.

Deprecation of the Codes of Conduct API preview

- The Codes of Conduct API preview, which was accessible with the `scarlet-witch-preview` header, is deprecated and no longer accessible in GitHub Enterprise Server 3.4. We instead recommend using the "[Get community profile metrics](#)" endpoint to retrieve information about a repository's code of conduct. For more information, see the "[Deprecation Notice: Codes of Conduct API preview](#)" in the GitHub changelog.

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

- Starting with GitHub Enterprise Server 3.4, the [deprecated version of the OAuth Application API endpoints](#) have been removed. If you encounter 404 error messages on these endpoints, convert your code to the versions of the OAuth Application API that do not have `access_tokens` in the URL. We've also disabled the use of API authentication using query parameters. We instead recommend using [API authentication in the request header](#).

Deprecation of the CodeQL runner

- The CodeQL runner is deprecated in GitHub Enterprise Server 3.4 and is no longer supported. The deprecation only affects users who use CodeQL code scanning in third party CI/CD systems; GitHub Actions users are not affected. We strongly recommend that customers migrate to the CodeQL CLI, which 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 deprecated in GitHub Enterprise Server 3.3 onwards.

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. For more information, see the [GitHub changelog](#). [Updated: 2022-06-14]

3.4.0: Backups

- GitHub Enterprise Server 3.4 requires at least [GitHub Enterprise Backup Utilities 3.4.0](#) for [Backups and Disaster Recovery](#).

3.4.0: Errata

- "[Encrypted secrets](#)" incorrectly indicated that secrets for GitHub Actions are encrypted in the instance's database. The article has been updated to reflect that secrets are not encrypted on the instance. To encrypt secrets at rest, you must encrypt your instance's block storage device. For more information, refer to the documentation for your hypervisor or cloud service. [Updated: 2023-06-01]

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)