

**This version of GitHub Enterprise was discontinued on 2022-10-12.** 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 3.2 release notes

# Enterprise Server 3.2.20

[Download GitHub Enterprise Server 3.2.20](#)

October 25, 2022

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

## Security fixes

- **HIGH:** Updated dependencies for the Management Console to the latest patch versions, which addresses security vulnerabilities including [CVE-2022-30123](#) and [CVE-2022-29181](#).
- **HIGH:** Added checks to address an improper cache key vulnerability that allowed an unauthorized actor to access private repository files through a public repository. This vulnerability has been assigned [CVE-2022-23738](#).
- **MEDIUM:** Updated [CommonMarker](#) to address a scenario where parallel requests to the Markdown REST API could result in unbounded resource exhaustion. This vulnerability has been assigned [CVE-2022-39209](#).
- **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.

## Bug fixes

- 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.

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories

are not included in GitHub.com search results.

- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.19

[Download GitHub Enterprise Server 3.2.19](#)

September 21, 2022

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

### Security fixes

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

### Bug fixes

- In a cluster configuration, running `ghe-cluster-config-apply` could cause unconfigured nodes to replicate configuration to the rest of the cluster, potentially removing configurations from existing nodes.
- In some cases, the Management Console's monitor dashboard would not load correctly.
- 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.
- After a user deleted or restored packages from the web interface, counts for packages could render incorrectly.
- Manually disabled GitHub Actions workflows in a repository were re-enabled if the repository received a push containing more than 2048 commits, or if the repository's default branch changed.

- When using a VPC endpoint URL as an AWS S3 URL for GitHub Packages, publication and installation of packages failed.

---

## Known issues

- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.18

[Download GitHub Enterprise Server 3.2.18](#)

August 30, 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.

---

## Bug fixes

- Duplicate administrative SSH keys could appear in both the Management Console and the `/home/admin/.ssh/authorized_keys` file.
- In some cases, background tasks could stall due to a library that was used concurrently despite not being thread-safe.

---

## Changes

- Generation of support bundles is faster as a result of parallelized log sanitization. For more information about support bundles, see "[Providing data to GitHub Support](#)."

---

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.17

August 11, 2022

[Download GitHub Enterprise Server 3.2.17](#)

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

---

## Security fixes

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

## Bug fixes

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

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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]

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

---

## Security fixes

- **MEDIUM:** Prevents an attack where a server-side request forgery (SSRF) could potentially force the Subversion (SVN) bridge to execute remote code by injecting arbitrary data into Memcached.
  - 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 vulnerability involving deserialization of untrusted data was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the Subversion (SVN) bridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2022-23734](#).
- 

## Bug fixes

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

## Changes

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

---

## Known issues

- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.15

June 28, 2022

[Download GitHub Enterprise Server 3.2.15](#)

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.

---

## Security fixes

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

---

## Bug fixes

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

## Changes

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

## Known issues

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

---



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

---

## Security fixes

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

## Bug fixes

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

## Changes

- Optimised the inclusion of metrics when generating a cluster support bundle.
  - In HA configurations where Elasticsearch reported a valid yellow status, changes introduced in a previous fix would block the `ghe-repl-stop` command and not allow replication to be stopped. Using `ghe-repo-stop --force` will now force Elasticsearch to stop when the service is in a normal or valid yellow status.
- 

## 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.

- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.13

[Download GitHub Enterprise Server 3.2.13](#)

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.

### Security fixes

- **MEDIUM:** A security issue in nginx resolver was identified, where an attacker who could forge UDP packets from the DNS server could cause 1-byte memory overwrite, resulting in worker process crashes or other potentially damaging impacts. The vulnerability has been assigned [CVE-2021-23017](#).
- Updated the `actions/checkout@v2` and `actions/checkout@v3` actions to address new vulnerabilities announced in the [Git security enforcement blog post](#).
- Packages have been updated to the latest security versions.

### Bug fixes

- In some cluster topologies, the `ghe-cluster-status` command left behind empty directories in `/tmp`.
- SNMP incorrectly logged a high number of `Cannot statfs` error messages to syslog.
- For instances configured with SAML authentication and built-in fallback enabled, built-in users would get stuck in a "login" loop when attempting to sign in from the page generated after logging out.

- Videos uploaded to issue comments would not be rendered properly.
  - When using SAML encrypted assertions, some assertions were not correctly marking SSH keys as verified.
  - When using `ghe-migrator`, a migration would fail to import video file attachments in issues and pull requests.
  - The Releases page would return a 500 error when the repository has tags that contain non-ASCII characters.
- [Updated: 2022-06-10]
- 

## Changes

- In high availability configurations, clarify that the replication overview page in the Management Console only displays the current replication configuration, not the current replication status.
  - When enabling GitHub Packages, clarify that using a Shared Access Signature (SAS) token as connection string is not currently supported.
  - Support bundles now include the row count of tables stored in MySQL.
  - Dependency Graph can now be enabled without vulnerability data, allowing you to see what dependencies are in use and at what versions. Enabling Dependency Graph without enabling GitHub Connect will **not** provide vulnerability information.
- 

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.12

[Download GitHub Enterprise Server 3.2.12](#)

April 20, 2022

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

---

## Security fixes

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

## Bug fixes

- Upgrading the nodes in a high availability pair with an upgrade package could cause Elasticsearch to enter an inconsistent state in some cases.
  - 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.
  - When converting a user account to an organization, if the user account was an owner of the GitHub Enterprise Server enterprise account, the converted organization would incorrectly appear in the enterprise owner list.
  - Creating an impersonation OAuth token using the Enterprise Administration REST API worked incorrectly when an integration matching the OAuth Application ID already existed.
- 

## Changes

- Configuration errors that halt a config apply run are now output to the terminal in addition to the configuration log.
  - When attempting to cache a value larger than the maximum allowed in Memcached, an error was raised however the key was not reported.
  - The CodeQL starter workflow no longer errors even if the default token permissions for GitHub Actions are not used.
  - If GitHub Advanced Security features are enabled on your instance, the performance of background jobs has improved when processing batches for repository contributions.
- 

## Known issues

- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.

- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.11

[Download GitHub Enterprise Server 3.2.11](#)

April 04, 2022

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

### Security fixes

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

## Bug fixes

- Minio processes would have high CPU usage if an old configuration option was present after upgrading GitHub Enterprise Server.
  - The options to enable `TLS 1.0` and `TLS 1.1` in the Privacy settings of the Management Console were shown, although removal of those protocol versions occurred in an earlier release.
  - In a HA environment, configuring MSSQL replication could require additional manual steps after enabling GitHub Actions for the first time.
  - A subset of internal configuration files are more reliably updated after a hotpatch.
  - The `ghe-run-migrations` script would sometimes fail to generate temporary certificate names correctly.
  - In a cluster environment, Git LFS operations could fail with failed internal API calls that crossed multiple web nodes.
  - Pre-receive hooks that used `gpg --import` timed out due to insufficient `syscall` privileges.
  - In some cluster topologies, webhook delivery information was not available.
  - In HA configurations, tearing down a replica would fail if GitHub Actions had previously been enabled.
  - Elasticsearch health checks would not allow a yellow cluster status when running migrations.
  - Organizations created as a result of a user transforming their user account into an organization were not added to the global enterprise account.
  - When using `ghe-migrator` or exporting from GitHub.com, a long-running export would fail when data was deleted mid-export.
  - The GitHub Actions deployment graph would display an error when rendering a pending job.
  - Links to inaccessible pages were removed.
  - Navigating away from a comparison of two commits in the web UI would have the diff persist in other pages.
  - 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 for a user](#) API endpoint would respond with an error when attempting to remove a member managed externally by a SCIM group.
  - A large number of dormant users could cause a GitHub Connect configuration to fail.
  - The "Feature & beta enrollments" page in the Site admin web UI was incorrectly available.
  - The "Site admin mode" link in the site footer did not change state when clicked.
  - The `spokesctl cache-policy rm` command no longer fails with the message `error: failed to delete cache policy`.
- 

## Changes

- Memcached connection limits were increased to better accommodate large cluster topologies.
- The Dependency Graph API previously ran with a statically defined port.
- The default shard counts for cluster-related Elasticsearch shard settings have been updated.

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

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.10

[Download GitHub Enterprise Server 3.2.10](#)

March 01, 2022

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

---

## Security fixes

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

---

## Bug fixes

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

---

## Known issues

- On a freshly set up GitHub Enterprise Server instance without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.9

February 17, 2022

[Download GitHub Enterprise Server 3.2.9](#)

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.

---



## Security fixes

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

## Bug fixes

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

## Changes

- Secret scanning will skip scanning ZIP and other archive files for secrets.
- 

## 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.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.8

[Download GitHub Enterprise Server 3.2.8](#)

February 01, 2022

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

---

## Security fixes

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

## Bug fixes

- Pages would become unavailable following a MySQL secret rotation until `nginx` was manually restarted.
  - Migrations could fail when GitHub Actions was enabled.
  - When setting the maintenance schedule with a ISO 8601 date, the actual scheduled time wouldn't match due to the timezone not being transformed to UTC.
  - Spurious error messages concerning the `cloud-config.service` would be output to the console.
  - The version number would not be correctly updated after a installing a hotpatch using `ghe-cluster-each`.
  - Webhook table cleanup jobs could run simultaneously, causing resource contention and increasing job run time.
  - When run from the primary, `ghe-repl-teardown` on a replica would not remove the replica from the MSSQL availability group.
  - When using CAS authentication and the "Reactivate suspended users" option was enabled, suspended users were not automatically reactivated.
  - The ability to limit email-based notifications to users with emails on a verified or approved domain did not work correctly.
  - A long-running database migration related to Security Alert settings could delay upgrade completion.
- 

## Changes

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

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.7

[Download GitHub Enterprise Server 3.2.7](#)

January 18, 2022

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

---

## Security fixes

- Packages have been updated to the latest security versions. In these updates, Log4j has been updated to version 2.17.1. Note: previous mitigations released in 3.3.1, 3.2.6, 3.1.14, and 3.0.22 are sufficient to address the impact of CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832 in these versions of GitHub Enterprise Server.
  - Sanitize more secrets in the generated support bundles
  - Packages have been updated to the latest security versions.
-

## Bug fixes

- Actions self hosted runners would fail to self-update or run new jobs after upgrading from an older GHES installation.
  - Storage settings could not be validated when configuring MinIO as blob storage for GitHub Packages.
  - Running `ghe-config-apply` could sometimes fail because of permission issues in `/data/user/tmp/pages`.
  - The save button in management console was unreachable by scrolling in lower resolution browsers.
  - IOPS and Storage Traffic monitoring graphs were not updating after collectd version upgrade.
  - Some webhook related jobs could generated large amount of logs.
  - Several documentation links resulted in a 404 Not Found error.
- 

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.6

December 13, 2021

[Download GitHub Enterprise Server 3.2.6](#)

This is not the [latest patch release](#) of this release series, and this is not the [latest release](#) of Enterprise Server. Please

use the latest release for the latest security, performance, and bug fixes.

---

## Security fixes

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

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.5

December 07, 2021

[Download GitHub Enterprise Server 3.2.5](#)

This is not the [latest patch release](#) of this release series, and this is not the [latest release](#) of Enterprise Server. Please

use the latest release for the latest security, performance, and bug fixes.

---

## Security fixes

- Support bundles could include sensitive files if they met a specific set of conditions.
  - A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.2.5, 3.1.13, 3.0.21. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2021-41598](#).
  - A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.0.21, 3.1.13, 3.2.5. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned [CVE-2021-41599](#). Updated February 17, 2022.
- 

## Bug fixes

- In some cases when Actions was not enabled, `ghe-support-bundle` reported an unexpected message `Unable to find MS SQL container.`
  - Running `ghe-config-apply` could sometimes fail because of permission issues in `/data/user/tmp/pages`.
  - A misconfiguration in the Management Console caused scheduling errors.
  - Docker would hold log files open after a log rotation.
  - Migrations could get stuck due to incorrect handling of `blob_path` values that are not UTF-8 compatible.
  - GraphQL requests did not set the `GITHUB_USER_IP` variable in pre-receive hook environments.
  - Pagination links on org audit logs would not persist query parameters.
  - During a hotpatch, it was possible for duplicate hashes if a transition ran more than once.
- 

## Changes

- Clarifies explanation of Actions path-style in documentation.
  - Updates support contact URLs to use the current support site, [support.github.com](https://support.github.com).
  - Additional troubleshooting provided when running `ghe-mssql-diagnostic`.
- 

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.4

[Download GitHub Enterprise Server 3.2.4](#)

November 23, 2021

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

---

Downloads have been disabled due to a major bug affecting multiple customers. A fix will be available in the next patch.

### Security fixes

- Packages have been updated to the latest security versions.

---

### Bug fixes

- Running `ghe-repl-start` or `ghe-repl-status` would sometimes return errors connecting to the database when GitHub Actions was enabled.
- Pre-receive hooks would fail due to undefined `PATH`.

- Running `ghe-repl-setup` would return an error: `cannot create directory /data/user/elasticsearch: File exists` if the instance had previously been configured as a replica.
  - Running `ghe-support-bundle` returned an error: `integer expression expected`.
  - After setting up a high availability replica, `ghe-repl-status` included an error in the output: `unexpected unclosed action in command`.
  - In large cluster environments, the authentication backend could be unavailable on a subset of frontend nodes.
  - Some critical services may not have been available on backend nodes in GHES Cluster.
  - The repository permissions to the user returned by the `/repos` API would not return the full list.
  - The `childTeams` connection on the `Team` object in the GraphQL schema produced incorrect results under some circumstances.
  - In a high availability configuration, repository maintenance always showed up as failed in stafftools, even when it succeeded.
  - User defined patterns would not detect secrets in files like `package.json` or `yarn.lock`.
- 

## Changes

- An additional outer layer of `gzip` compression when creating a cluster support bundle with `ghe-cluster-support-bundle` is now turned off by default. This outer compression can optionally be applied with the `ghe-cluster-support-bundle -c` command line option.
  - We have added extra text to the admin console to remind users about the mobile apps' data collection for experience improvement purposes.
  - The GitHub Connect data connection record now includes a list of enabled GitHub Connect features. [Updated 2021-12-09]
- 

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.3

[Download GitHub Enterprise Server 3.2.3](#)

November 09, 2021

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

---

### Security fixes

- A path traversal vulnerability was identified in GitHub Pages builds on GitHub Enterprise Server that could allow an attacker to read system files. To exploit this vulnerability, an attacker needed permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3, and was fixed in versions 3.0.19, 3.1.11, and 3.2.3. This vulnerability was reported through the GitHub Bug Bounty program and has been assigned CVE-2021-22870.
  - Packages have been updated to the latest security versions.
- 

### Bug fixes

- Some Git operations failed after upgrading a GitHub Enterprise Server 3.x cluster because of the HAProxy configuration.
- Unicorn worker counts might have been set incorrectly in clustering mode.
- Resqued worker counts might have been set incorrectly in clustering mode.
- If Ubuntu's Uncomplicated Firewall (UFW) status was inactive, a client could not clearly see it in the logs.
- Upgrading from GitHub Enterprise Server 2.x to 3.x failed when there were UTF8 characters in an LDAP configuration.
- Some pages and Git-related background jobs might not run in cluster mode with certain cluster configurations.
- The documentation link for Server Statistics was broken.
- When a new tag was created, the [push](#) webhook payload did not display a correct `head_commit` object. Now, when a new tag is created, the push webhook payload now always includes a `head_commit` object that contains the data of the commit that the new tag points to. As a result, the `head_commit` object will always contain the commit data of the payload's `after` commit.
- The enterprise audit log page would not display audit events for secret scanning.

- There was an insufficient job timeout for replica repairs.
  - A repository's releases page would return a 500 error when viewing releases.
  - Users were not warned about potentially dangerous bidirectional unicode characters when viewing files. For more information, see "[Warning about bidirectional Unicode text](#)" in the GitHub Blog.
  - Hookshot Go sent distribution type metrics that Collectd could not handle, which caused a ballooning of parsing errors.
  - Public repositories displayed unexpected results from secret scanning with a type of `Unknown Token`.
- 

## Changes

- Kafka configuration improvements have been added. When deleting repositories, package files are now immediately deleted from storage account to free up space. `DestroyDeletedPackageVersionsJob` now deletes package files from storage account for stale packages along with metadata records.
- 

## Known issues

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.2

[Download GitHub Enterprise Server 3.2.2](#)

October 28, 2021

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

---

## Security fixes

- It was possible for cleartext passwords to end up in certain log files.
  - Several known weak SSH public keys have been added to the deny list and can no longer be registered. In addition, versions of GitKraken known to generate weak SSH keys (7.6.x, 7.7.x and 8.0.0) have been blocked from registering new public keys.
  - Packages have been updated to the latest security versions.
- 

## Bug fixes

- Restore might fail for enterprise server in clustering mode if orchestrator is not healthily.
  - Codespaces links were displayed in organization settings.
  - Several parts of the application were unusable for users who are owners of many organizations.
  - Fixed a link to <https://docs.github.com>.
- 

## Changes

- Browsing and job performance optimizations for repositories with many refs.
- 

## Known issues

- After saving a new release on a repository, the `/releases` page shows a 500 error. A fix for this issue is expected to ship in 3.2.3.
- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files [uploaded through the web interface](#) are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories

are not included in GitHub.com search results.

- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- Resource limits that are specific to processing pre-receive hooks may cause some pre-receive hooks to fail.
- 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 3.2.1

[Download GitHub Enterprise Server 3.2.1](#)

October 12, 2021

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

### Security fixes

- Packages have been updated to the latest security versions.

### Bug fixes

- Custom pre-receive hooks could have failed due to too restrictive virtual memory or CPU time limits.
- In a GitHub Enterprise Server clustering configuration, Dependency Graph settings could have been incorrectly applied.
- Attempting to wipe all existing configuration settings with `ghe-cleanup-settings` failed to restart the Management Console service.
- During replication teardown via `ghe-repl-teardown` Memcached failed to be restarted.
- During periods of high load, users would receive HTTP 503 status codes when upstream services failed internal healthchecks.
- Pre-receive hook environments were forbidden from calling the `cat` command via BusyBox on Alpine.
- Failing over from a primary Cluster datacenter to a secondary Cluster datacenter succeeds, but then failing back over to the original primary Cluster datacenter failed to promote Elasticsearch indices.

- The "Import teams" button on the Teams page for an Organization returned an HTTP 404.
  - Using the API to disable Secret Scanning correctly disabled the property but incorrectly returned an HTTP 422 and an error message.
  - In some cases, GitHub Enterprise Administrators attempting to view the `Dormant users` page received `502 Bad Gateway` or `504 Gateway Timeout` response.
  - Performance was negatively impacted in certain high load situations as a result of the increased number of `SynchronizePullRequestJob` jobs.
  - A user defined pattern created for Secret Scanning would continue getting scanned even after it was deleted.
- 

## Changes

- GitHub Apps now set the Secret Scanning feature on a repository consistently with the API.
- 

## Known issues

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

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](#)."

## Features

### Custom patterns for secret scanning

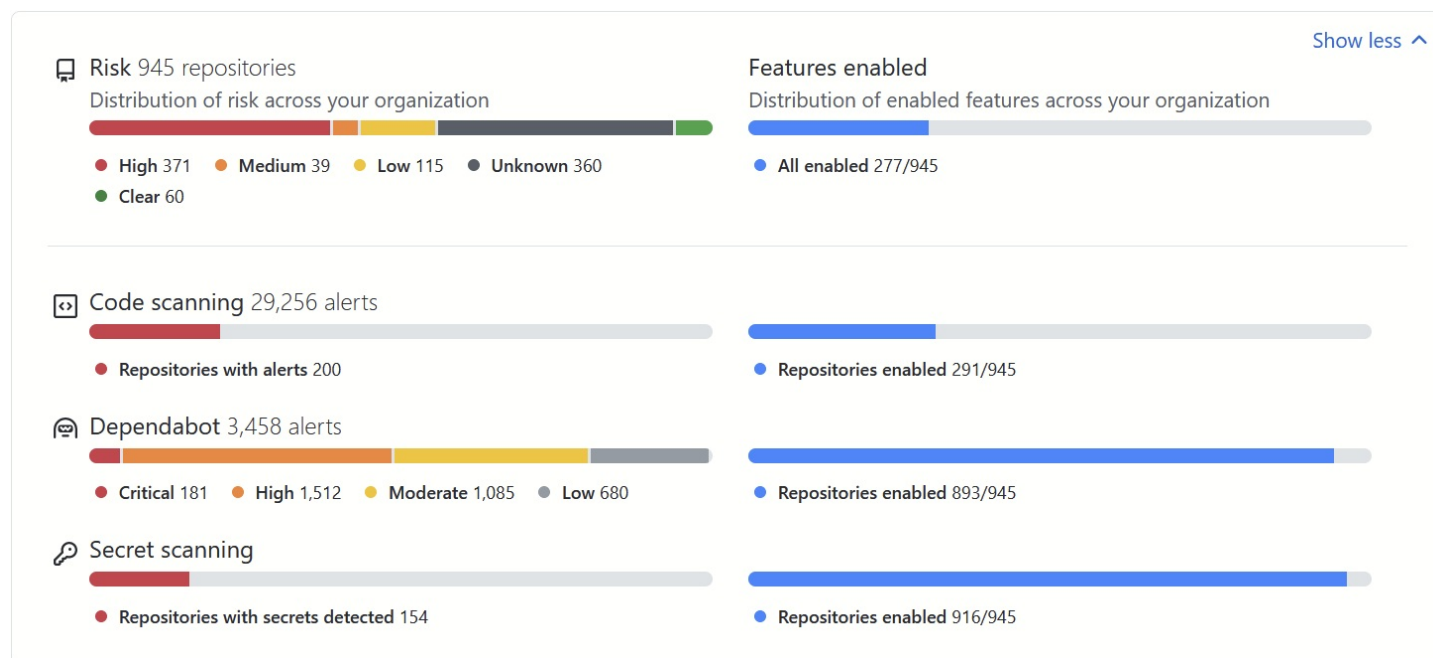
- GitHub Advanced Security customers can now specify custom patterns for secret scanning. When a new pattern is specified, secret scanning searches a repository's entire Git history for the pattern, as well as any new commits.

User defined patterns are in beta for GitHub Enterprise Server 3.2. They can be defined at the repository, organization, and enterprise levels. For more information, see "[Defining custom patterns for secret scanning](#)."

### Security overview for Advanced Security (beta)

- GitHub Advanced Security customers now have an organization-level view of the application security risks detected by code scanning, Dependabot, and secret scanning. The security overview shows the enablement status of security features on each repository, as well as the number of alerts detected.

In addition, the security overview lists all secret scanning alerts at the organization level. Similar views for Dependabot and code scanning alerts are coming in future releases. For more information, see "[About the security overview](#)."



### Dependency review (beta)

- GitHub Advanced Security customers can now see a rich diff of the dependencies changed in a pull request. Dependency review provides an easy-to-understand view of dependency changes and their security impact in the "Files changed" tab of pull requests. It informs you of which dependencies were added, removed, or updated, along with vulnerability information for these dependencies. For more information, see "[Reviewing dependency changes in a pull request](#)."

### GitHub Actions environments



## Approving unverified domains for email notifications

- Domains that are not able to be verified can now be approved for email notification routing. Enterprise and organization owners will be able to approve domains and immediately augment their email notification restriction policy, allowing notifications to be sent to collaborators, consultants, acquisitions, or other partners. For more information, see "[Verifying or approving a domain for your enterprise](#)" and "[Restricting email notifications for your enterprise](#)."

## Git Credential Manager (GCM) secure credential storage and multi-factor authentication support

- Git Credential Manager (GCM) versions 2.0.452 and later now provide security-hardened credential storage and multi-factor authentication support for GitHub Enterprise Server.

GCM with support for GitHub Enterprise Server is included with [Git for Windows](#) versions 2.32 and later. GCM is not included with Git for macOS or Linux, but can be installed separately. For more information, see the [latest release](#) and [installation instructions](#) in the `GitCredentialManager/git-credential-manager` repository.

---

## Changes

### Administration Changes


- A 'User Agent Referrer Policy' setting has been added to the enterprise settings. This allows an admin to set a stricter `Referrer-Policy` to hide the hostname of a GitHub Enterprise Server installation from external sites. The setting is disabled by default and is tracked by audit log events for staff and enterprise owners when enabled or disabled. For more information, see "[Configuring Referrer Policy for your enterprise](#)."
- The MySQL health check was changed to use `mysqladmin ping` instead of TCP checks, which removes some unnecessary noise in the MySQL error log. Also, Orchestrator failover checks were improved to prevent unnecessary MySQL failovers when applying cluster config changes.
- The Resque service, which supports background job processing, has been replaced with Aqueduct Lite. This change makes the job system easier to manage and should not affect the user experience. For the new administration and debugging commands for Aqueduct, see "[Command-line utilities](#)."

### Token Changes

- The format of authentication tokens for GitHub Enterprise Server has changed. The change affects the format of personal access tokens and access tokens for OAuth Apps, as well as user-to-server, server-to-server, and refresh tokens for GitHub Apps.

The different token types now have unique identifiable prefixes, which allows for secret scanning to detect the tokens so that you can mitigate the impact of someone accidentally committing a token to a repository. GitHub recommends updating existing tokens as soon as possible. For more information, see "[About authentication to GitHub](#)" and "[About secret scanning](#)."

### Repositories changes

- Repositories on user profiles and organization profiles now support sorting by star count.
- When viewing the commit history of a single file, you can now click  to view that file at the selected point in history.
- When a submodule is defined with a relative path in your GitHub Enterprise Server instance, the submodule is now clickable in the web UI. Clicking the submodule in the web UI will take you to the linked repository. Previously, only submodules with absolute URLs were clickable. This is supported for relative paths for repositories with the same owner that follow the pattern `../REPOSITORY` or relative paths for repositories with a different owner that follow the



pattern `../OWNER/REPOSITORY`. For more information about working with submodules, see [Working with submodules](#) on the GitHub Blog.

- The web UI can now be used to synchronize an out-of-date branch of a fork with the fork's upstream branch. If there are no merge conflicts between the branches, the branch is updated either by fast-forwarding or by merging from upstream. If there are conflicts, you will be prompted to create a pull request to resolve the conflicts. For more information, see "[Syncing a fork](#)."

## Markdown changes

- The markdown editor used when creating or editing a release in a repository now has a text-editing toolbar. For more information, see "[Managing releases in a repository](#)."
- Uploading video files is now supported everywhere you write Markdown on GitHub Enterprise Server. Share demos, reproduction steps, and more in your issue and pull request comments, as well as in Markdown files within repositories, such as READMEs. For more information, see "[Attaching files](#)."
- Markdown files will now automatically generate a table of contents in the header when there are 2 or more headings. The table of contents is interactive and links to the selected section. All 6 Markdown heading levels are supported.
- There is a new keyboard shortcut, `cmd+e` on macOS or `ctrl+e` on Windows, to insert codeblocks in Markdown files, issues, pull requests, and comments.
- Appending `?plain=1` to the URL for any Markdown file will now display the file without rendering and with line numbers. The plain view can be used to link other users to specific lines. For example, appending `?plain=1#L52` will highlight line 52 of a plain text Markdown file. For more information, see "[Creating a permanent link to a code snippet](#)."

## Issues and pull requests changes

- With the [latest version of Octicons](#), the states of issues and pull requests are now more visually distinct so you can scan their status more easily. For more information, see [the GitHub Blog](#).
- A new "Require conversation resolution before merging" branch protection rule and "Conversations" menu is now available. Easily discover your pull request comments from the "Files changed" tab, and require that all your pull request conversations are resolved before merging. For more information, see "[About pull request reviews](#)" and "[About protected branches](#)."
- To prevent the merge of unexpected changes after auto-merge is enabled for a pull request, auto-merge is now disabled automatically when new changes are pushed by a user without write access to the repository. Users without write access can still update the pull request with changes from the base branch when auto-merge is enabled. To prevent a malicious user from using a merge conflict to introduce unexpected changes to the pull request, auto-merge for the pull request is disabled if the update causes a merge conflict. For more information about auto-merge, see "[Automatically merging a pull request](#)."
- People with maintain permissions can now manage the repository-level "Allow auto-merge" setting. This setting, which is off by default, controls whether auto-merge is available on pull requests in the repository. Previously, only people with admin permissions could manage this setting. Additionally, this setting can now be controlled using the "[Create a repository](#)" and "[Update a repository](#)" REST APIs. For more information, see "[Managing auto-merge for pull requests in your repository](#)."
- The assignees selection for issues and pull requests now supports type ahead searching so you can find users in your organization faster. Additionally, search result rankings have been updated to prefer matches at the start of a person's username or profile name.
- When a review is requested from a team of more than 100 people, developers are now shown a confirmation dialog box in order to prevent unnecessary notifications for large teams.
- Back-tick `code blocks` are now supported in issue titles, pull request titles, and in any place issue and pull request titles are referenced in GitHub Enterprise Server.
- Events for pull requests and pull request reviews are now included in the audit log for both [enterprises](#) and [organizations](#). These events help admins better monitor pull request activity and help ensure security and

compliance requirements are being met. Events can be viewed from the web UI, exported as CSV or JSON, or accessed via REST API. You can also search the audit log for specific pull request events. For more information, see "[Reviewing the audit log for your organization](#)."

## Branches changes

- The default branch name for new repositories is now `main`. Existing repositories are not impacted by this change. If users, organization owners, or enterprise owners have previously specified a default branch for new repositories, they are also not impacted.

If you want to set a different default branch name, you can do so in the [user](#), [organization](#), or [enterprise](#) settings.

- Branches, including the default branch, can now be renamed using the the GitHub Enterprise Server web UI. When a branch is renamed, any open pull requests and draft releases targeting the renamed branch will be retargeted automatically, and branch protection rules that explicitly reference the renamed branch will be updated.

Admin permissions are required to rename the default branch, but write permissions are sufficient to rename other branches.

To help make the change as seamless as possible for users:

- A notice is shown to contributors, maintainers, and admins on the repository homepage with instructions for updating their local repository.
- Web requests to the old branch will be redirected.
- A "moved permanently" HTTP response will be returned to REST API calls.
- An informational message is displayed to Git command line users that push to the old branch.

For more information, see "[Renaming a branch](#)."

## GitHub Actions changes

- GitHub Actions now lets you control the permissions granted to the `GITHUB_TOKEN` secret. The `GITHUB_TOKEN` is an automatically-generated secret that lets you make authenticated calls to the API for GitHub Enterprise Server in your workflow runs. GitHub Actions generates a new token for each job and expires the token when a job completes. The token usually has `write` permissions to a number of [API endpoints](#), except in the case of pull requests from forks, which are always `read`. These new settings allow you to follow a principle of least privilege in your workflows. For more information, see "[Authentication in a workflow](#)."
- GitHub CLI 1.9 and later allows you to work with GitHub Actions in your terminal. For more information, see the [GitHub changelog](#).
- The audit log now includes events associated with GitHub Actions workflow runs. This data provides administrators with a greatly expanded data set for security and compliance audits. For more information, see "[Reviewing the audit log for your organization](#)."
- GitHub Enterprise Server 3.2 contains performance improvements for job concurrency with GitHub Actions. For more information about the new performance targets for a range of CPU and memory configurations, see "[Getting started with GitHub Actions for GitHub Enterprise Server](#)".
  - The "Maximum Concurrency" values were modified to reflect our most up to date performance testing. [Updated: 2021-12-07]
- The [GitHub Actions Runner](#) application in GitHub Enterprise Server 3.2 has been updated to [v2.279.0](#).

## GitHub Packages changes

- Any package or package version for GitHub Packages can now be deleted from GitHub Enterprise Server's web UI. You can also undo the deletion of any package or package version within 30 days. For more information, see "[Deleting and restoring a package](#)".

## Dependabot and Dependency graph changes

- The dependency graph can now be enabled using the Management Console, rather than needing to run a command in the administrative shell. For more information, see "[Enabling alerts for vulnerable dependencies GitHub Enterprise Server](#)."
- Notifications for multiple Dependabot alerts are now grouped together if they're discovered at the same time. This significantly reduces the volume of Dependabot alert notifications that users receive. For more information, see the [GitHub changelog](#).
- Dependency graph and Dependabot alerts now support Go modules. GitHub Enterprise Server analyzes a repository's `go.mod` files to understand the repository's dependencies. Along with security advisories, the dependency graph provides the information needed to alert developers to vulnerable dependencies. For more information about enabling the dependency graph on private repositories, see "[Securing your repository](#)."
- The default notification settings for security alerts have changed. Previously, if you had permission to view security alerts in a repository, you would receive notifications for that repository as long as your settings allowed for security alert notifications. Now, you must opt in to security alert notifications by watching the repository. You will be notified if you select `All Activity` or configure `Custom` to include `Security alerts`. All existing repositories will be automatically migrated to these new settings and you will continue to receive notifications; however, any new repositories will require opting-in by watching the repository. For more information see "[Configuring notifications for Dependabot alerts](#)" and "[Managing alerts from secret scanning](#)."

### Code scanning and secret scanning changes

- Code scanning with CodeQL now generates diagnostic information for all supported languages. This helps check the state of the created database to understand the status and quality of performed analysis. The diagnostic information is available starting in [version 2.5.6](#) of the [CodeQL CLI](#). You can see the detailed diagnostic information in the GitHub Actions logs for CodeQL. For more information, see "[Viewing code scanning logs](#)."
- Code scanning with CodeQL CLI now supports analyzing several languages during a single build. This makes it easier to run code analysis to use CI/CD systems other than GitHub Actions. The new mode of the `codeql` database `create` command is available starting [version 2.5.6](#) of the [CodeQL CLI](#). For more information about setting this up, see "[Installing CodeQL CLI in your CI system](#)."
- Code scanning alerts from all enabled tools are now shown in one consolidated list, so that you can easily prioritize across all alerts. You can view alerts from a specific tool by using the "Tool" filter, and the "Rule" and "Tag" filters will dynamically update based on your "Tool" selection.
- Code scanning with CodeQL now includes beta support for analyzing C++20 code. This is only available when building codebases with GCC on Linux. C++20 modules are not supported yet.
- The depth of CodeQL's analysis has been improved by adding support for more [libraries and frameworks](#) and increasing the coverage of our existing library and framework models for several languages ([C++](#), [JavaScript](#), [Python](#), and [Java](#)). As a result, CodeQL can now detect even more potential sources of untrusted user data, review the steps through which that data flows, and identify potentially dangerous sinks in which this data could end up. This results in an overall improvement of the quality of the code scanning alerts. For more information, see the [GitHub changelog](#).
- Code scanning now shows `security-severity` levels for CodeQL security alerts. You can configure which `security-severity` levels will cause a check failure for a pull request. The severity level of security alerts can be `critical`, `high`, `medium`, or `low`. By default, any code scanning alerts with a `security-severity` of `critical` or `high` will cause a pull request check failure.

Additionally, you can now also configure which severity levels will cause a pull request check to fail for non-security alerts. You can configure this behavior at the repository level, and define whether alerts with the severity `error`, `warning`, or `note` will cause a pull request check to fail. By default, non-security code scanning alerts with a severity of `error` will cause a pull request check failure.

For more information see "[Defining which alert severity levels cause pull request check failure](#)."

<input type="checkbox"/>	<b>Hard-coded credentials</b> <span>Critical</span>	main
	spec/node-spec.js#L381 • Detected on 15 Jun by CodeQL	
<input type="checkbox"/>	<b>Hard-coded credentials</b> <span>Critical</span>	main
	spec/node-spec.js#L377 • Detected on 15 Jun by CodeQL	
<input type="checkbox"/>	<b>Hard-coded credentials</b> <span>Critical</span>	main
	spec/fixtures/pages/basic-auth.html#L11 • Detected on 15 Jun by CodeQL	
<input type="checkbox"/>	<b>Unvalidated dynamic method call</b> <span>High</span>	main
	spec-main/fixtures/extensions/chrome-api/main.js#L45 • Detected on 15 Jun by CodeQL	
<input type="checkbox"/>	<b>Unvalidated dynamic method call</b> <span>High</span>	main
	spec-main/api-net-spec.ts#L84 • Detected on 15 Jun by CodeQL	

- Improvements to the branch filter for code scanning alerts make it clearer which code scanning alerts are being displayed on the alerts page. By default, code scanning alerts are filtered to show alerts for the default branch of the repository only. You can use the branch filter to display the alerts on any of the non-default branches. Any branch filter that has been applied is shown in the search bar.

The search syntax has also been simplified to `branch:<branch name>`. This syntax can be used multiple times in the search bar to filter on multiple branches. The previous syntax, `ref:refs/heads/<branch name>`, is still supported, so any saved URLs will continue to work.

- Free text search is now available for code scanning alerts. You can search code scanning results to quickly find specific alerts without having to know exact search terms. The search is applied across the alert's name, description, and help text. The syntax is:
  - A single word returns all matches.
  - Multiple search words returns matches to either word.
  - Words in double quotes returns exact matches.
  - The keyword 'AND' returns matches to multiple words.
- Secret scanning added patterns for 23 new service providers. For the updated list of supported secrets, see "[About secret scanning](#)."

## API Changes

- Pagination support has been added to the Repositories REST API's "compare two commits" endpoint, which returns a list of commits reachable from one commit or branch, but unreachable from another. The API can also now return the results for comparisons over 250 commits. For more information, see the "[Commits](#)" REST API documentation and "[Traversing with pagination](#)."
- The REST API can now be used to programmatically resend or check the status of webhooks. For more information, see "[Repositories](#)," "[Organizations](#)," and "[Apps](#)" in the REST API documentation.
- Improvements have been made to the code scanning and GitHub Advanced Security APIs:
  - The code scanning API now returns the CodeQL query version used for an analysis. This can be used to reproduce results or confirm that an analysis used the latest query. For more information, see "[Code scanning](#)" in the REST API documentation.
  - Admin users can now use the REST API to enable or disable GitHub Advanced Security for repositories, using the `security_and_analysis` object on `repos/{org}/{repo}`. In addition, admin users can check whether Advanced Security is currently enabled for a repository by using a `GET /repos/{owner}/{repo}` request. These changes help you manage Advanced Security repository access at scale. For more information, see "[Repositories](#)" in the REST API documentation.

## Known issues

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

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

---

## Deprecations

### Deprecation of GitHub Enterprise Server 2.21

- **GitHub Enterprise Server 2.21 was discontinued on June 6, 2021.** That 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 2.22

- **GitHub Enterprise Server 2.22 will be discontinued on September 23, 2021.** That 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

- Beginning in GitHub Enterprise Server 3.1, we will begin discontinuing support for Xen Hypervisor. The complete deprecation is scheduled for GitHub Enterprise Server 3.3, following the standard one year deprecation window. Please contact [GitHub Support](#) with questions or concerns.

### Removal of Legacy GitHub Services

- GitHub Enterprise Server 3.2 removes unused GitHub Service database records. More information is available in the [deprecation announcement post](#).

### Deprecation of OAuth Application API endpoints and API authentication via query parameters

- To prevent accidental logging or exposure of `access_tokens`, we discourage the use of OAuth Application API endpoints and the use of API auth via query params. Visit the following posts to see the proposed replacements:

- [Replacement OAuth Application API endpoints](#)
- [Replacement auth via headers instead of query param](#)

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

### Removal of legacy GitHub App webhook events and endpoints

- Two legacy GitHub Apps-related webhook events have been removed: `integration_installation` and `integration_installation_repositories`. You should instead be listening to the `installation` and `installation_repositories` events.
- The following REST API endpoint has been removed: `POST /installations/{installation_id}/access_tokens`. You should instead be using the namespaced equivalent `POST /app/installations/{installation_id}/access_tokens`.

### Change to the format of authentication tokens affects GitHub Connect

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

---

## Backups

- GitHub Enterprise Server 3.2 requires at least [GitHub Enterprise Backup Utilities 3.2.0](#) for [Backups and Disaster Recovery](#).