This version of GitHub Enterprise was discontinued on 2022-06-03. 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 3.1 release notes

Enterprise Server 3.1.22

Download GitHub Enterprise Server 3.1.22

June 09, 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

- 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 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

- 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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.21

Download GitHub Enterprise Server 3.1.21

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.
- When using SAML encrypted assertions, some assertions were not correctly marking SSH keys as verified.
- 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 supported.
- Support bundles now include the row count of tables stored in MySQL.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.20

Download GitHub Enterprise Server 3.1.20

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.
- The `maint_host_low` job queues were not processed, resulting in some maintenance tasks failing to run.
- When converting a user account to an organization, if the user account was an owner of the GitHub Enterprise Server enterprise account, the converted organization would incorrectly appear in the enterprise owner list.
- Creating an impersonation OAuth token using the Enterprise Administration REST API resulted in an error when an integration matching the OAuth Application ID already existed.

Changes

- When attempting to cache a value larger than the maximum allowed in Memcached, an error was raised however the key was not reported.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.19

Download GitHub Enterprise Server 3.1.19

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

- 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.
- Links to inaccessible pages were removed.
- Adding a team as a reviewer to a pull request would sometimes show the incorrect number of members on that team.
- 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.

Changes

- Memcached connection limits were increased to better accommodate large cluster topologies.
- More effectively identify and delete webhook logs that are outside of the webhook log retention window.
- 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.
- `NotProcessedError` exceptions were occurring unnecessarily.
- Performance has been improved for web requests made by enterprise owners.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.18

Download GitHub Enterprise Server 3.1.18

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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.17

Download GitHub Enterprise Server 3.1.17

February 17, 2022

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

Security fixes

- Packages have been updated to the latest security versions.

Bug fixes

- Fixes SystemStackError (stack too deep) when getting more than 2^16 keys from memcached.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.16

Download GitHub Enterprise Server 3.1.16

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.
- 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 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.
- Several documentation links resulted in a 404 Not Found error.

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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.15

Download GitHub Enterprise Server 3.1.15

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

- 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.

- The repository permissions to the user returned by the `/repos` API would not return the full list.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.14

Download GitHub Enterprise Server 3.1.14

December 13, 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

- ⚠ **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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.13

Download GitHub Enterprise Server 3.1.13

December 07, 2021

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

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

- 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.
- GraphQL requests did not set the GITHUB_USER_IP variable in pre-receive hook environments.

Changes

- Clarifies explanation of Actions path-style in documentation.
- Updates support contact URLs to use the current support site, support.github.com.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.12

Download GitHub Enterprise Server 3.1.12

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.

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.
- 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.

Changes

- An additional outer layer of `gzip` compression when creating a cluster support bundle with `ghe-cluster-suport-bundle` is now turned off by default. This outer compression can optionally be applied with the `ghe-cluster-suport-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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.11

Download GitHub Enterprise Server 3.1.11

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.
- 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.
- 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.

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

- 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.

- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.10

Download GitHub Enterprise Server 3.1.10

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 isnt healthily.

- 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

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.9

Download GitHub Enterprise Server 3.1.9

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.
- 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.
- With Actions configured, MSSQL replication would fail after restoring from a GitHub Enterprise Backup Utilities snapshot.
- An erroneous `jq` error message may have been displayed when running `ghe-config-apply`.
- Pre-receive hook environments were forbidden from calling the cat command via BusyBox on Alpine.
- The external database password was logged in plaintext.
- 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 indicies.
- The "Import teams" button on the Teams page for an Organization returned an HTTP 404.
- 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.

Changes

- More effectively delete Webhook logs that fall out of the Webhook log retention window.

Known issues

- 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.

- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.8

Download GitHub Enterprise Server 3.1.8

September 24, 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

- **HIGH:** A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This is the result of an incomplete fix for CVE-2021-22867. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned CVE-2021-22868.
- **MEDIUM:** An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in 3.0.16 and 3.1.8 releases. It has been assigned CVE-2021-22869.

Bug fixes

- Resque worker counts were displayed incorrectly during maintenance mode.
- Allocated memcached memory could be zero in clustering mode.
- Non-empty binary files displayed an incorrect file type and size on the pull request "Files" tab.
- Fixes GitHub Pages builds so they take into account the NO_PROXY setting of the appliance. This is relevant to appliances configured with an HTTP proxy only. (update 2021-09-30)
- The GitHub Connect configuration of the source instance was always restored to new instances even when the `--config` option for `ghe-restore` was not used. This would lead to a conflict with the GitHub Connect connection and license synchronization if both the source and destination instances were online at the same time. The fix also requires updating backup-utils to 3.2.0 or higher. [updated: 2021-11-18]

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.7

Download GitHub Enterprise Server 3.1.7

September 07, 2021

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

Security fixes

- Packages have been updated to the latest security versions.

Bug fixes

- Attempting to tear down a newly-added replica node by specifying its UUID with `ghe-repl-teardown` would fail without reporting an error if replication was not started.
- GitHub Pages builds were being passed through an external proxy if there was one configured.
- Custom pre-receive hooks that created sub-processes would lack a `PATH` variable in their environment, resulting in "No such file or directory" errors.
- MySQL could failover during an upgrade if `mysql-auto-failover` was enabled.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.6

Download GitHub Enterprise Server 3.1.6

August 24, 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

- Attaching very large images or animated GIFs to images or pull requests would fail.
- Journald messages related to automatic updates (`Adding h/m/s random time.`) were logged to syslog.
- Custom pre-receive hooks that created named pipes (FIFOs) would crash or hang, resulting in a timeout error.
- Adding filters to the audit log advanced search page did not populate the query text box in real-time with the correct facet prefix and value.
- Git hooks to the internal API that result in failing requests returned the exception `undefined method body for "success":String (NoMethodError)` instead of returning an explicit `nil`.
- When an integration was removed, it was possible for an unrelated OAuth application or integration to also be removed.
- When a mandatory message containing an emoji character was added, attempting to view or change the message would return a 500 Internal Server Error.

Changes

- Adds `triage` and `maintain` to the list of permissions returned by the REST API.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.5

Download GitHub Enterprise Server 3.1.5

August 10, 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.

Bug fixes

- Custom pre-receive hooks that used a bash subshell would return an error: `No such file or directory`.
- When GitHub Actions is enabled without running regular scheduled backups the MSSQL Transaction Log could grow unbounded and can consume all available space on the appliance's Data Disk causing a possible outage.
- Unnecessary database logging consumed a large amount of disk space on instances with heavy LFS usage.
- Audit log entries for changes made to "Repository creation" organization settings were inaccurate.

- Excessive logging of `ActionController::UnknownFormat` exceptions caused unnecessary disk usage.
- LDAP `group_dn` values longer than 255 characters would result in errors being logged: `Data truncated for column 'group_dn' at row 1`.

Changes

- Abuse rate limits are now called Secondary rate limits, since the behavior they limit is not always abusive.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.4

Download GitHub Enterprise Server 3.1.4

July 27, 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

- The counts on packages pages were not being incremented when a package was downloaded.
- `ghe-config-apply` would timeout, ask for a prompt or fail for a customer that had secret scanning enabled, and had either disabled or never enabled GitHub Actions on their instance.
- Log files were not reopened after rotation in some cases leading to high disk space usage on instances with high uptime.
- Upgrade could fail from older version of GitHub Enterprise Server due to a missing job in GitHub Actions.
- Custom pre-receive hooks could lead to an error like `error: object directory /data/user/repositories/0/nw/12/34/56/7890/network.git/objects does not exist; check .git/objects/info/alternates`.
- Unauthenticated HTTP proxy for the pages containers build was not supported for any users that use HTTP proxies.
- A significant number of 503 errors were logged every time a user visited a repository's `/settings` page if the dependency graph was not enabled.
- Internal repositories were only returned when a user had affiliations with the repository through a team or through collaborator status, or queried with the `?type=internal` parameter.
- Failed background jobs had unlimited retries which could cause large queue depths.
- A significant number of 503 errors were being created if the scheduled job to sync vulnerabilities with GitHub.com attempted to run when dependency graph was not enabled and content analysis was enabled.
- When GitHub Actions is enabled without running regular scheduled backups, the MSSQL transaction log could grow unbounded and can consume all available space on the appliance's data disk, causing a possible outage.

  If you have configured regularly scheduled MSSQL backups, no further actions is required. Otherwise, if you have GitHub Actions previously enabled, run the following commands after installing this patch.

  ```
  ghe-actions-console -s Mps -c 'Update-Service -Force'
  ghe-actions-console -s Token -c 'Update-Service -Force'
  ghe-actions-console -s Actions -c 'Update-Service -Force'
  ```

Changes

- The logs for `babeld` now include a `cmd` field for HTTP ref advertisement requests instead of only including it during the negotiation requests.

Known issues

- 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.
- 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.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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 a direct upgrade to 3.4 on your upgrade path 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: 2022-09-12]

Enterprise Server 3.1.3

Download GitHub Enterprise Server 3.1.3

July 14, 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

- **HIGH:** A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.3 and has been assigned CVE-2021-22867. This vulnerability was reported via the GitHub Bug Bounty program.

- Packages have been updated to the latest security versions.

Bug fixes

- SAML expiration date variable was not configurable.
- Application services would fail their health checks during config apply before they could enter a healthy state.
- `ghe-cluster-config-node-init` would fail during cluster setup if HTTP proxy is enabled.
- Pre-receive hooks could encounter an error `Failed to resolve full path of the current executable` due to `/proc` not being mounted on the container.
- Collectd would not resolve the forwarding destination hostname after the initial startup.
- The job that purged stale deleted repositories could fail to make progress if some of those repositories were protected from deletion by legal holds.
- Background jobs were being queued to the `spam` queue which were not being processed.
- The preferred merge method would be reset when retrying after a failed PR merge.
- Git pushes could result in a 500 Internal Server Error during the user reconciliation process on instances using LDAP authentication mode.
- After upgrading from 3.0.x to 3.1.x, in some cases GitHub Actions would fail with an error: `An unexpected error occurred when executing this workflow.`

Changes

- Improved the efficiency of config apply by skipping IP allow firewall rules that had not changed, which saved significant time on large clusters.

Known issues

- 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.
- 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.

- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.2

Download GitHub Enterprise Server 3.1.2

June 24, 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

- A large number of `gauge-dependency-graph-api-dispatch_dispatch` metrics could accumulate in the Management Console.
- The sshd service would sometimes fail to start on instances running on Google Cloud Platform.
- Old upgrade files would persist on the user disk, sometimes resulting in out of space conditions.
- `gh-migrator` displayed an incorrect path to its log output.
- An export archive would silently fail to import pull requests if they contained review requests from teams not present in the archive.

Changes

- Update the GitHub Actions Runner version in GHES 3.1 to v2.278.0

Known issues

- 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.
- 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.
- After upgrading from 3.0.x to 3.1.x, in some cases GitHub Actions can fail with an error: `An unexpected error occurred when executing this workflow.` To workaround this problem, connect to the administrative shell (ssh) and run:

  ```
  ghe-actions-console -s actions -c "Queue-ServiceJob -JobId 4DB1F4CF-19FD-40E0-A253-91288813DE8B"
  ```

- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.1

Download GitHub Enterprise Server 3.1.1

June 10, 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

- SVN 1.7 and older clients showed an error when using the `svn co` and `svn export` commands.
- Accessing a repository through the administrative shell using `ghe-repo <owner>/<reponame>` would hang.
- After upgrading, users experienced reduced availability during heavy usage, because services restarted too frequently. This would occur due to timeout mismatches between the nomad configuration and that of the internal services.
- In some instances, running `ghe-repl-status` after setting up GitHub Actions would produce an error and `ghe-actions-teardown` would fail.
- `ghe-dbconsole` would return errors under some circumstances.
- Import failures of organizations or repositories from non-GitHub sources could produce an `undefined method '[]' for nil:NilClass` error.
- GitHub profile names might have changed unintentionally when using SAML authentication, if the GitHub profile name did not match the value of the attribute mapped to the `Full name` field in the Management Console.
- Upgrading an instance that had previously ran a 2.13 release, but not a 2.14 release, resulted in a database migration error relating to the `AddRepositoryIdToCheckRuns` data transition.

Changes

- Users of the GraphQL API can query the public field `closingIssuesReferences` on the `PullRequest` object. This field retrieves issues that will be automatically closed when the related pull request is merged. This approach will also allow this data to be migrated in future, as part of a higher fidelity migration process.

Known issues

- 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.
- 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.
- After upgrading from 3.0.x to 3.1.x, in some cases GitHub Actions can fail with an error: `An unexpected error occurred when executing this workflow.` To workaround this problem, connect to the administrative shell (ssh) and run:

  ```
  ghe-actions-console -s actions -c "Queue-ServiceJob -JobId 4DB1F4CF-19FD-40E0-A253-91288813DE8B"
  ```

- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.
- If GitHub Actions is enabled for GitHub Enterprise Server, teardown of a replica node with `ghe-repl-teardown` will succeed, but may return `ERROR:Running migrations`.
- 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: 2022-09-12]

Enterprise Server 3.1.0

Download GitHub Enterprise Server 3.1.0

June 03, 2021

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

For minimum infrastructure requirements, see "About minimum requirements for GitHub Enterprise Server 3.0 and later."

Features

GitHub Advanced Security Secret Scanning

- Secret Scanning is now generally available on GitHub Enterprise Server 3.1+. Scan public and private repositories for committed credentials, find secrets, and notify the secret provider or admin the moment they are committed into a repository.

  This release includes several improvements from the beta of Secret Scanning on GitHub Enterprise Server:

  - Expanded our pattern coverage from 24 partners to 37
  - Added an API and webhooks
  - Added notifications for commit authors when they commit secrets
  - Updated the index view to made it easy to triage secrets in bulk

- Reduced the false positive rate on many patterns

Administrators using GitHub Advanced Security can enable and configure GitHub Advanced Security secret scanning. You can review the updated minimum requirements for your platform before you turn on GitHub Advanced Security secret scanning.

GitHub Advanced Security billing improvements

- This release includes several improvements to GitHub Advanced Security billing in GitHub Enterprise Server:
  - GitHub Advanced Security customers can now view their active committer count and the remaining number of unused committer seats on their organization or enterprise account's Billing page. If Advanced Security is purchased for an enterprise, administrators can also view the active committer seats which are being used by other organizations within their enterprise. For more information, see "About GitHub Advanced Security licensing" and "Viewing your GitHub Advanced Security usage."
  - GitHub Advanced Security customers can now view their active committer count for any Advanced Security enabled repositories on their organization or enterprise account's Billing page. These changes help billing administrators track their usage against how many committer licenses they purchased. For more information see "Managing security and analysis settings for your organization."

Dependabot improvements

- This release includes improvements to Dependabot alerts in GitHub Enterprise Server:
  - Users with Dependabot alerts enabled can see which of their repositories are impacted by a given vulnerability by navigating to its entry in the GitHub Advisory Database. This feature is available in public beta. For more information, see "Viewing and updating vulnerable dependencies in your repository."
  - When a vulnerability is added to GitHub Advisory Database, you will no longer receive email and web notifications for Dependabot alerts on low and moderate severity vulnerabilities. These alerts are still accessible from the repository's Security tab. For more information, see "Viewing and updating vulnerable dependencies in your repository."
  - You can now give people instructions on how to responsibly report security vulnerabilities in your project by adding a `SECURITY.md` file to your repository's `root`, `docs`, or `.github` folder. When someone creates an issue in your repository, they will see a link to your project's security policy. For more information, see "Adding a security policy to your repository."

GitHub Actions Workflow Visualization beta

- GitHub Actions can now generate a visual graph of your workflow on every run. With workflow visualization, you can:
  - View and understand complex workflows
  - Track progress of workflows in real-time
  - Troubleshoot runs quickly by easily accessing logs and jobs metadata
  - Monitor progress of deployment jobs and easily access deployment targets

  For more information, see "Using the visualization graph."

OAuth 2.0 Device Authorization Grant

- OAuth 2.0 Device Authorization Grant allows any CLI client or developer tool to authenticate using a secondary system with a browser.

  Administrators using OAuth Apps and GitHub Apps can enable and configure OAuth 2.0 Device Authorization Flow, in addition to the existing Web Application Flow. You can review the updated minimum requirements for your platform before you enable OAuth 2.0 Device Authorization Flow.

Pull request auto-merge

- With auto-merge, pull requests can be set to merge automatically when all merge requirements have been satisfied. This saves users from needing to constantly check the state of their pull requests just to merge them. Auto-merge can be enabled by a user with permission to merge and on pull requests that have unsatisfied merge requirements. For more information, see "Automatically merging a pull request."

Custom notifications

- You can customize the types of notifications you want to receive from individual repositories. For more information, see "Configuring notifications."

GitHub Mobile filtering

- GitHub Mobile filtering allows you to search for and find issues, pull requests, and discussions from your device. New metadata for issues and pull request list items allow you to filter by assignees, checks status, review states, and comment counts.

  GitHub Mobile beta is available for GitHub Enterprise Server. Sign in with our Android and iOS apps to triage notifications and manage issues and pull requests on the go. Administrators can disable mobile support for their Enterprise using the management console or by running `ghe-config app.mobile.enabled false`. For more information, see "GitHub Mobile."

Changes

Administration Changes

- By precomputing checksums, the amount of time a repository is under the lock has reduced dramatically, allowing more write operations to succeed immediately and improving monorepo performance.
- The latest release of the CodeQL CLI supports uploading analysis results to GitHub. This makes it easier to run code analysis for customers who wish to use CI/CD systems other than GitHub Actions. Previously, such users had to use the separate CodeQL runner, which will continue to be available. For more information, see "About CodeQL code scanning in your CI system."
- GitHub Actions now supports skipping `push` and `pull_request` workflows by looking for some common keywords in your commit message.
- Check annotations older than four months will be archived.
- Scaling of worker allocation for background tasks has been revised. We recommend validating that the new defaults are appropriate for your workload. Custom background worker overrides should be unset in most cases. [Updated 2022-03-18]

Security Changes

- Following feedback, display of Code Scanning results on a pull request without submitting with a pull request ID will remain supported. For more information, see "Configuring code scanning" and "Configuring CodeQL code scanning in your CI system.
- SARIF upload support increased to a maximum of 5000 results per upload.

Developer Changes

- You can specify multiple callback URLs while configuring a GitHub App. This can be used in services with multiple domains or subdomains. GitHub will always deny authorization if the callback URL from the request is not in the authorization callback URL list.

- The GitHub App file permission has been updated to allow an app developer to specify up to 10 files for read-only or read-write access that their app can request access to.
- CodeQL now supports more libraries and frameworks for a variety of languages (C++, JavaScript, Python,Java, Go). The CodeQL engine can now detect more sources of untrusted user data, which improves the quality and depth of the code scanning alerts. For more information, see "About CodeQL."
- When configuring a GitHub App, the authorization callback URL is a required field. Now, we allow the developer to specify multiple callback URLs. This can be used in services with multiple domains or subdomains. GitHub will always deny authorization if the callback URL from the request is not in the authorization callback URL list.
- Delete an entire directory of files, including subdirectories, from your web browser. For more information, see "Deleting a file or directory."
- Include multiple words after the `#` in an issue, discussion, or pull request comment to further narrow your search.
- When you're writing an issue, pull request, or discussion comment the list syntax for bullets, numbers, and tasks autocompletes after you press `return` or `enter`.

API Changes

- The code scanning API allows users to upload data about static analysis security testing results, or export data about alerts. For more information, see the code scanning API reference.
- The GitHub Apps API for managing installations has now graduated from an API preview to a generally available API. The preview header is no longer required to access these endpoints.

Security fixes

- **MEDIUM** Under certain circumstances, users who were removed from a team or organization could retain write access to branches they had existing pull requests opened for.
- Packages have been updated to the latest security versions.

Bug fixes

Fixes for known issues from Release Candidate

- All known issues from Release Candidate 1 have been fixed, except those listed in the Known Issues section below.

Fixes for other issues

- On the "Configure Actions and Packages" page of the initial installation process, clicking on the "Test domain settings" button did not complete the test.
- Running `ghe-btop` failed with an error and cannot find a `babeld` container.
- MySQL could reload and cause downtime if you change auto failover settings.
- After upgrading, a mismatch of internal and external timeout values created service unavailability.
- Expected replication delays in MSSQL generated warnings.

- Link to "Configuring clustering" on the Management Console was incorrect.
- When creating or editing a pre-receive hook, a race condition in the user interface meant that after selecting a repository, files within the repository were sometimes not populated in files dropdown.
- When an IP address is added to a whitelist using "Create Whitelist Entry" button, it could still be shown as locked out.
- References to the "Dependency graph" and "Dependabot alerts" features were not shown as disabled on some repositories.
- Setting an announcement in the enterprise account settings could result in a 500 Internal Server Error.
- HTTP POST requests to the `/hooks` endpoint could fail with a 401 response due to an incorrectly configured `hookID`.
- The `build-server` process failed to clean up processes, leaving them in the `defunct` state.
- `spokesd` created excessive log entries, including the phrase "fixing placement skipped".
- While upgrading Actions the upgrade could fail if the instance could not make self-requests via its configured hostname.
- Upgrading from 2.22.x to 3.1.0.rc1 could result in a database migration error relating to the `BackfillIntegrationApplicationCallbackUrlsTransition` data transition.

Known issues

- Access to a repository through the administrative shell using `ghe-repo <owner>/<reponame>` will hang. As a workaround, use `ghe-repo <owner>/<reponame> -c "bash -i"` until a fix is available in the next version.
- 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.
- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- 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 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.
- Upgrading an instance that has previously ran a 2.13 release, but not a 2.14 release, results in a database migration error relating to the `AddRepositoryIdToCheckRuns` data transition.
- After upgrading from 3.0.x to 3.1.x, in some cases GitHub Actions can fail with an error: `An unexpected error occurred when executing this workflow.` To workaround this problem, connect to the administrative shell (ssh) and run:

  ```
  ghe-actions-console -s actions -c "Queue-ServiceJob -JobId 4DB1F4CF-19FD-40E0-A253-91288813DE8B"
  ```

- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

- 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: 2022-09-12]

Deprecations

Deprecation of GitHub Enterprise Server 2.20

- **GitHub Enterprise Server 2.20 was discontinued on March 2, 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 2.21

- **GitHub Enterprise Server 2.21 will be discontinued on June 9, 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 Legacy GitHub App Webhook Events

- Starting with GitHub Enterprise Server 2.21.0 two legacy GitHub Apps-related webhook events have been deprecated and will be removed in GitHub Enterprise Server 3.2.0. The deprecated events `integration_installation` and `integration_installation_repositories` have equivalent events which will be supported. More information is available in the deprecation announcement blog post.

Deprecation of Legacy GitHub Apps Endpoint

- Starting with GitHub Enterprise Server 2.21.0 the legacy GitHub Apps endpoint for creating installation access tokens was deprecated and will be removed in GitHub Enterprise Server 3.2.0. More information is available in the deprecation announcement blog post.

Deprecation of OAuth Application API

- GitHub no longer supports the OAuth application endpoints that contain `access_token` as a path parameter. We have introduced new endpoints that allow you to securely manage tokens for OAuth Apps by moving `access_token` to the request body. While deprecated, the endpoints are still accessible in this version. We intend to remove these endpoints on GitHub Enterprise Server 3.4. For more information, see the deprecation announcement blog post.

Deprecation of GitHub Actions short SHA support

- GitHub Actions will remove support for referencing actions using the shortened version of a git commit SHA. This may cause some workflows in your repository to break. To fix these workflows, you will need to update the action reference to use the full commit SHA. For more information, see "Security hardening for GitHub Actions."

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.

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 3.1 requires at least GitHub Enterprise Backup Utilities 3.1.0 for Backups and Disaster Recovery.
