This version of GitHub Enterprise was discontinued on 2022-02-16. 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 3.0 release notes

Enterprise Server 3.0.25

Download GitHub Enterprise Server 3.0.25

February 17, 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.

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.
- 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.

Enterprise Server 3.0.24

Download GitHub Enterprise Server 3.0.24

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.
- The version number would not be correctly updated after a installing a hotpatch using `ghe-cluster-each`.
- Spurious error messages concerning the `cloud-config.service` would be output to the console.
- When using CAS authentication and the "Reactivate suspended users" option was enabled, suspended users were not automatically reactivated.

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.
- 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.

Enterprise Server 3.0.23

Download GitHub Enterprise Server 3.0.23

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.

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.
- 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.

Enterprise Server 3.0.22

Download GitHub Enterprise Server 3.0.22

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

- 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.
- 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.

Enterprise Server 3.0.21

Download GitHub Enterprise Server 3.0.21

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

- 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.
- 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.

Enterprise Server 3.0.20

Download GitHub Enterprise Server 3.0.20

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

- 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.
- 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

- 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.
- 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.

Enterprise Server 3.0.19

Download GitHub Enterprise Server 3.0.19

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.
- Some pages and Git-related background jobs might not run in cluster mode with certain cluster configurations.
- The enterprise audit log page would not display audit events for secret scanning.
- 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`.

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.
- 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.

Enterprise Server 3.0.18

Download GitHub Enterprise Server 3.0.18

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

- 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

- Several parts of the application were unusable for users who are owners of many organizations.

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.
- 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.

Enterprise Server 3.0.17

Download GitHub Enterprise Server 3.0.17

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.
- Pre-receive hook environments were forbidden from calling the cat command via BusyBox on Alpine.
- The external database password was logged in plaintext.
- An erroneous `jq` error message may have been displayed when running `ghe-config-apply`.
- 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 Site Admin page for repository self-hosted runners returned an HTTP 500.
- In some cases, GitHub Enterprise Administrators attempting to view the `Dormant users` page received `502 Bad Gateway` or `504 Gateway Timeout` response.

Changes

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

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.
- 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.

Enterprise Server 3.0.16

Download GitHub Enterprise Server 3.0.16

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.
- 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

- 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.
- 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.

Enterprise Server 3.0.15

Download GitHub Enterprise Server 3.0.15

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

- 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.
- 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.

Enterprise Server 3.0.14

Download GitHub Enterprise Server 3.0.14

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 used a bash subshell would return an error: `No such file or directory`.
- 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.

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.
- 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.

Enterprise Server 3.0.13

Download GitHub Enterprise Server 3.0.13

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

- 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.
- 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

- 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.
- 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.

Enterprise Server 3.0.12

Download GitHub Enterprise Server 3.0.12

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

- 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.

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

- 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.
- 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.

Enterprise Server 3.0.11

Download GitHub Enterprise Server 3.0.11

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.
- Running `git nw-gc --pristine` would result in an error.
- 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.

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

- 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.
- 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.

Enterprise Server 3.0.10

Download GitHub Enterprise Server 3.0.10

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.
- Log rotation could sometimes interrupt background jobs.
- `gh-migrator` displayed an incorrect path to its log output.
- An export archive would fail to import if it contained review requests from teams not present in the archive.

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.
- 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.

Enterprise Server 3.0.9

Download GitHub Enterprise Server 3.0.9

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

- The upgrade process could fail while upgrading Actions if the instance could not make self-requests using its configured hostname.
- 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.

Changes

- The `firstPatchedVersion` field is now available on `SecurityVulnerability` objects in the GraphQL API.
- 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

- 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.
- 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.

Enterprise Server 3.0.8

Download GitHub Enterprise Server 3.0.8

May 25, 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

- **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

- On the "Configure Actions and Packages" page of the initial installation process, when an admin clicked the "Test domain settings" button the test did not complete.
- Running `ghe-btop` failed with error `cannot find a 'babeld' container`.
- Users were experiencing service unavailability after upgrading due to a mismatch of internal and external timeout values.
- Normal replication delays in MSSQL generated warnings.
- Link for GitHub Enterprise Clustering Guide on management console was incorrect.
- An IP address added by an admin using the "Create Whitelist Entry" button could still be locked out.
- References to the "Dependency graph" and "Dependabot alerts" features were shown on repositories where they were not enabled.
- HTTP POST requests to the `/hooks` endpoint could fail with a 401 response due to the `hookID` being set incorrectly.
- 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".

Changes

- Check annotations older than 4 months will be archived.

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.
- 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.
- 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.

Enterprise Server 3.0.7

Download GitHub Enterprise Server 3.0.7

May 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

- **HIGH:** 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. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. All permissions being granted would properly be shown during the first authorization, but in certain circumstances, if the user revisits the authorization flow after the GitHub App has configured additional user-level permissions, those additional permissions may not be shown, leading to more permissions being granted than the user potentially intended. This vulnerability affected GitHub Enterprise Server 3.0.x prior to 3.0.7 and 2.22.x prior to 2.22.13. It was fixed in versions 3.0.7 and 2.22.13. This vulnerability has been assigned CVE-2021-22866 and was reported via the GitHub Bug Bounty Program.
- Packages have been updated to the latest security versions.

Bug fixes

- Quotes included in Actions or Packages storage configuration could cause errors.
- Custom pre-receive hooks could fail due to too restrictive file size or number of open file limits.
- Orchestrator auto failover could be enabled during the phase of config apply.
- Users with maintainer permissions to a repository were shown an e-mail verification warning instead of a successful page build on the repository Pages settings page.
- The code owner of a wildcard rule would be incorrectly added to the list of owners for the code owners badge even if a later rule took precedence for that path.
- OpenAPI documentation referred to an invalid header.
- 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.

Changes

- Added logging for config change on HAProxy reload.
- Added logging for repository creation.

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 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.
- 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.

Enterprise Server 3.0.6

Download GitHub Enterprise Server 3.0.6

April 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

- Packages have been updated to the latest security versions.

Bug fixes

- During upgrades, the process would pause indefinitely after `cleanup nomad job`.
- Failing `ghe-cluster-failover` with the error message `Trilogy::Error: trilogy_connect`.

- `ghe-cluster-status-mysql` showed warnings about failovers as errors.
- Setup script running on MySQL replication may have caused unnecessary database reseeding during database failover.
- Upgrades did not include the latest version of Actions runner properly installed.
- `github-env` configuration could result in zombie processes.
- `config-apply` could take longer than necessary due to `rake db:migrate` being called unnecessarily.
- Orchestrator could have failed over to a MySQL replica which was not replicating from primary during seeding phase when primary could not be connected.
- Organizations or projects with errors blocked migration and could not be excluded.
- The Create Repository button was disabled for users who belonged to more than 50 organizations.
- Deleting a branch would temporarily flash an error message indicating something went wrong when the deletion was successful.
- The `rms-packages` index was shown in the site admin dashboard.
- Organization owner was unable to create internal repository due to the correct visibility options not being displayed on the form.
- The repository actions tab rendered a 500 in cases where the actions starter workflows were misconfigured.
- Customers with more than three storage hosts were unable to restore to their disaster-recovery cluster due to the fullest disks being selected instead of empty nodes.
- Code Scanning backend services did not start up reliably after applying hotpatches.

Changes

- Preflight checks allow all AWS instance types by default.

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 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.
- 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.

Enterprise Server 3.0.5

Download GitHub Enterprise Server 3.0.5

April 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.

The minimum infrastructure requirements have increased for GitHub Enterprise Server 3.0+. For more information, see "About minimum requirements for GitHub Enterprise Server 3.0 and later."

Security fixes

- Packages have been updated to the latest security versions.

Bug fixes

- Some logs were not included in the log forwarding configuration.
- A warning message `jq: error (at <stdin>:0): Cannot index number with string "settings"` could occur during replica promotion.
- Continuously restoring backups to a cluster could fail due to MySQL replicas failing to connect to the primary.
- Pages were not getting published when using custom CA certificate.
- Packages related subdomains were not showing up in the "Test domain settings" prompt for subdomain isolation.
- The `X-GitHub-Enterprise-Host` header sent with webhooks included a random string, rather than the hostname of the GitHub Enterprise Server instance that sent the HTTP POST payload.
- Upgrading from 2.22.x to 3.0.x would fail if GitHub Actions had previously been enabled, but disabled before the upgrade.
- Visiting the `/settings/emails` page would store state that could cause improper redirects when logging out and logging back in.
- GitHub integration apps were not able to notify teams when mentioned directly via an at-mention in an issue comment.
- reStructuredText (RST) rendering in the web UI would fail and instead displayed raw RST markup text.
- Email notifications for Secret Scanning alerts were not sent to authorized users when the Dependency Graph was not fully enabled.
- When ghe-migrator encountered import errors, it would sometimes abort the entire process, and the logs did not include enough context.
- Jupyter notebooks with non-ASCII characters could fail to render.

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 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.
- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- 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.

Enterprise Server 3.0.4

Download GitHub Enterprise Server 3.0.4

April 01, 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.

The minimum infrastructure requirements have increased for GitHub Enterprise Server 3.0+. For more information, see "About minimum requirements for GitHub Enterprise Server 3.0 and later."

Security fixes

- **HIGH:** An improper access control vulnerability was identified in GitHub Enterprise Server that allowed access tokens generated from a GitHub App's web authentication flow to read private repository metadata via the REST API without having been granted the appropriate permissions. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. The private repository metadata returned would be limited to repositories owned by the user the token identifies. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.4 and was fixed in versions 3.0.4, 2.22.10, 2.21.18. This vulnerability has been assigned CVE-2021-22865 and was reported via the GitHub Bug Bounty Program.
- Packages have been updated to the latest security versions.

Bug fixes

- When maintenance mode was enabled, some services continued to be listed as "active processes" even though they were expected to be running, and should not have been listed.
- After upgrading from 2.22.x to 3.0.x with GitHub Actions enabled, the self-hosted runner version was not updated and no self-hosted updates were made.
- Old GitHub Pages builds were not cleaned up leading to increased disk usage.
- `memcached` was not running on active replicas.
- Upgrade failed when updating file permissions when GitHub Actions was enabled.
- A timezone set on GitHub Enterprise 11.10.x or earlier was not being used by some services which were defaulting to UTC time.
- Services were not transitioning to new log files as part of log rotation, resulting in increased disk usage.
- The `ghe-saml-mapping-csv` command-line utility produced a warning message.
- The label on search results for internal repositories was shown as "Private" instead of "Internal".

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 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.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non-ASCII UTF-8 characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- 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.

Enterprise Server 3.0.3

Enterprise Server 3.0.3

Download GitHub Enterprise Server 3.0.3

March 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

- **HIGH:** A remote code execution 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 override environment variables leading to code execution 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 3.0.3 and was fixed in 3.0.3, 2.22.9, and 2.21.17. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned CVE-2021-22864.
- Packages have been updated to the latest security versions.

Bug fixes

- Running `ghe-cluster-config-init` could cause a cluster to become inoperable.
- Resolving merge conflicts in the GUI would fail when custom pre-receive hooks are configured on the repository.
- `launch-deployer` and `launch-receiver` were logging at DEBUG level and filling logs with unnecessary information.
- Systemd could lose track of HAProxy's PID.
- When Actions was configured to use S3 storage, the logs for an action would sometimes fail to load.
- The mysql-failover warning was displayed indefinitely after a successful failover.
- The `ghe-cluster-config-init` run was not fully accounting for the exit code of background jobs leading to improper handling of preflight checks.
- When enabling GitHub Actions, initialization could fail silently.
- When vulnerability alerting is enabled, upgrades to the 3.0 series would fail.
- Jobs related to Codespaces were being enqueued leading to an accumulation of unprocessed jobs.

Changes

- Use a relative number for consul and nomad `bootstrap_expect` allowing for a cluster to bootstrap even if a handful of nodes are down.
- Logs will rotate based on size in addition to time.

- Added kafka-lite to the `ghe-cluster-status` command.

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 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.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non-ASCII UTF-8 characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- Old builds of Pages are not cleaned up, which could fill up the user disk (`/data/user/`).
- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- Log rotation may fail to signal services to transition to new log files, leading to older log files continuing to be used, and eventual root disk space exhaustion. To remedy and/or prevent this issue, run the following commands in the administrative shell (SSH), or contact GitHub Enterprise Support for assistance:

```
printf "PATH=/usr/local/sbin:/usr/local/bin:/usr/local/share/enterprise:/usr/sbin:/usr/bin:/sbin:/bin\n29,59
sudo /usr/sbin/logrotate -f /etc/logrotate.conf
```

- 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.

Enterprise Server 3.0.2

Download GitHub Enterprise Server 3.0.2

March 16, 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.

The minimum infrastructure requirements have increased for GitHub Enterprise Server 3.0+. For more information, see

"About minimum requirements for GitHub Enterprise Server 3.0 and later."

Security fixes

- Packages have been updated to the latest security versions.

Bug fixes

- During a backup an error "Warning: One or more storage objects were not found on the source appliance." was occurring when attempting to clean up purgeable storage objects.
- Dependency graph failed to parse `yarn.lock` JavaScript manifest files, resulting in HTTP 500 errors in logs.
- Disabling GitHub Actions would sometimes fail.
- Custom pre-receive hooks weren't allowed to write to `/tmp`, preventing some scripts from running correctly.
- Systemd journal logs were duplicated in multiple places.
- A timezone set on GitHub Enterprise 11.10.x or earlier was reset to UTC time after upgrading to 3.0 which caused timestamps to shift in some instances.
- Clicking "Publish your first package" in the packages sidebar on a repository would lead to an empty page.
- A site admin could get a 500 error page while trying to view issues referenced from private repositories.
- After disabling GitHub Packages, some organization pages would return an HTTP 500 error response.
- Importing of repository archives from GitHub Enterprise Server that are missing repository files would fail with an error.
- Repository deploy keys were unable to be used with repositories containing LFS objects.
- In the packages sidebar of a repository, the Docker icon was gray and a tool tip displayed "This service is deprecated".
- Webhooks configured with a content type of `application/x-www-form-urlencoded` did not receive query parameters in the POST request body.
- Users could dismiss a mandatory message without checking all checkboxes.
- In some cases after upgrading from a 2.22.X instance, the web interface assets were missing and the page would not render correctly.
- Running `ghe-config-apply` could time out with `Failure waiting for nomad jobs to apply` due to `'job' stanza not found`.

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 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.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non-ASCII UTF-8 characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- Old builds of Pages are not cleaned up, which could fill up the user disk (`/data/user/`).
- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- Users may experience assets such as avatars not loading, or a failure to push/pull code. This may be caused by a PID mismatch in the `haproxy-cluster-proxy` service. To determine if you have an affected instance:

  Single instance

  1. Run this in the administrative shell (SSH):

     ```
     if [ $(cat /var/run/haproxy-cluster-proxy.pid) -ne $(systemctl show --property MainPID --value haproxy-c
     ```

  2. If it shows that there is a mismatch, reboot the instance.

  Cluster or High Availability configuration

  1. Run this in the administrative shell (SSH):

     ```
     ghe-cluster-each -- 'if [ $(cat /var/run/haproxy-cluster-proxy.pid) -ne $(systemctl show --property Main
     ```

  2. If it shows one or more nodes are affected, reboot the affected nodes.

- 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.

Enterprise Server 3.0.1

Download GitHub Enterprise Server 3.0.1

March 02, 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.

The minimum infrastructure requirements have increased for GitHub Enterprise Server 3.0+. For more information, see "About minimum requirements for GitHub Enterprise Server 3.0 and later."

Security fixes

- **HIGH:** An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to gain write access to unauthorized repositories via specifically crafted pull requests and REST API requests. An attacker would need to be able to fork the targeted repository, a setting that is disabled by default for organization owned private repositories. Branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability has been assigned CVE-2021-22861. This issue was reported via the GitHub Bug Bounty Program.
- **HIGH:** An improper access control vulnerability was identified in the GitHub Enterprise Server GraphQL API that allowed authenticated users of the instance to modify the maintainer collaboration permission of a pull request without proper authorization. By exploiting this vulnerability, an attacker would be able to gain access to head branches of pull requests opened on repositories of which they are a maintainer. Forking is disabled by default for organization owned private repositories and would prevent this vulnerability. Additionally, branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability has been assigned CVE-2021-22863. This issue was reported via the GitHub Bug Bounty Program.
- **HIGH:** An improper access control vulnerability was identified in GitHub Enterprise Server that allowed an authenticated user with the ability to fork a repository to disclose Actions secrets for the parent repository of the fork. This vulnerability existed due to a flaw that allowed the base reference of a pull request to be updated to point to an arbitrary SHA or another pull request outside of the fork repository. By establishing this incorrect reference in a PR, the restrictions that limit the Actions secrets sent a workflow from forks could be bypassed. This vulnerability affected GitHub Enterprise Server versions 3.0.0, 3.0.0.rc2, and 3.0.0.rc1 and has been assigned CVE-2021-22862. This vulnerability was reported via the GitHub Bug Bounty program.
- **MEDIUM:** GitHub Tokens from GitHub Pages builds could end up in logs.
- Packages have been updated to the latest security versions.

Bug fixes

- The load-balancer health checks in some cases could cause the babeld logs to fill up with errors about the PROXY protocol.
- The HTTP headers were not compliant with HTTP RFC standards in specific responses like 304 status for archives.
- On instances that host Python repositories with the Dependency Graph feature enabled, the instance could become unresponsive due to the root disk filling with error logs.
- An informational message was unintentionally logged as an error during GitHub Enterprise Backup Utilities snapshots, which resulted in unnecessary emails being sent when backups were scheduled by cron jobs that listen for output to stderr.
- On VMWare ESX 6.7 the initial configuration could hang while creating host keys which left the instance inaccessible via SSH.
- When GitHub Actions was enabled, disabling maintenance mode in the management console failed.

- The Package creation setting was shown on the organization member settings page, though this feature is not yet available.
- While enabling secret scanning on the Security & Analysis page the dialog incorrectly mentions private repositories.
- When editing a wiki page a user could experience a 500 error when clicking the Save button.
- An S/MIME signed commit using a certificate with multiple names in the subject alternative name would incorrectly show as "Unverified" in the commit badge.
- User saw 500 error when executing git operations on an instance configured with LDAP authentication.
- Suspended user was sent emails when added to a team.
- When a repository had a large number of manifests an error `You have reached the maximum number of allowed manifest files (20) for this repository.` was shown on the Insights -> Dependency graph tab. For more information, see Visualization limits.
- Fixes users being shown the option to set up the Code Scanning CodeQL Action even if Actions was not enabled for their repository.
- The "Prevent repository admins from changing anonymous Git read access" checkbox available in the enterprise account settings could not be successfully enabled or disabled.
- The modal used to display a mandatory message contained no vertical scrollbar, meaning longer messages could not be viewed in full.
- Redis would sometimes fail to start after a hard reboot or application crash.
- Dependency graph fails to parse `setup.py` Python manifest files, resulting in HTTP 500 errors in logs. This, combined with the duplicated logging issue, results in increased root volume utilization.

Changes

- Satisfy requests concurrently when multiple users are downloading the same archive, resulting in improved performance.

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 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.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support.
- Duplicated logging to `/var/log/messages`, `/var/log/syslog`, and `/var/log/user.log` results in increased root

volume utilization.

- Users can dismiss a mandatory message without checking all checkboxes.
- Pre-receive hook scripts cannot write temporary files, which may cause script execution to fail. Users who use pre-receive hooks should test in a staging environment to see if scripts require write access.
- Repository deploy keys are unable to be used with repositories containing LFS objects.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non-ASCII UTF-8 characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- Dependency graph fails to parse `yarn.lock` Javascript manifest files, resulting in HTTP 500 errors in logs.
- Instances with a custom timezone that were upgraded from an earlier release of GitHub Enterprise Server may have incorrect timestamps in the web UI.
- Old builds of Pages are not cleaned up, which could fill up the user disk (`/data/user/`).
- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- Users may experience assets such as avatars not loading, or a failure to push/pull code. This may be caused by a PID mismatch in the `haproxy-cluster-proxy` service. To determine if you have an affected instance:

  Single instance

  1. Run this in the administrative shell (SSH):

     ```
     if [ $(cat /var/run/haproxy-cluster-proxy.pid) -ne $(systemctl show --property MainPID --value haproxy-c
     ```

  2. If it shows that there is a mismatch, reboot the instance.

  Cluster or High Availability configuration

  1. Run this in the administrative shell (SSH):

     ```
     ghe-cluster-each -- 'if [ $(cat /var/run/haproxy-cluster-proxy.pid) -ne $(systemctl show --property Main
     ```

  2. If it shows one or more nodes are affected, reboot the affected nodes.

- 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.

Enterprise Server 3.0.0

February 16, 2021

Download GitHub Enterprise Server 3.0.0

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.

The minimum infrastructure requirements have increased for GitHub Enterprise Server 3.0+. For more information, see "About minimum requirements for GitHub Enterprise Server 3.0 and later."

Security fixes

- **HIGH:** A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands 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 has been assigned CVE-2020-10519 and was reported via the GitHub Bug Bounty Program.

Features

GitHub Actions

- GitHub Actions is now generally available on GitHub Enterprise Server 3.0+. Build, test, and deploy your code from GitHub. Submit code reviews, branch management, and issue triaging work the way you want.

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

  - Enterprise, organization, and repository admins can create security policies for access to GitHub Actions on GitHub.com.
  - Enterprise, organization, and repository admins can allow public repositories to use self-hosted runners.
  - Enterprise, organization, and repository admins can now allow workflows to run on pull requests raised from forks of private repositories.
  - The `workflow_run` event is now supported
  - Users now have the ability to disable workflows and enable them at a later date.
  - Workflow logs have been enhanced for a better user experience.
  - Users can now use private images in container jobs and services.
  - The max retention days for artifacts and logs can now be customized.
  - The runner group API now includes labels.
  - You can now create reusable actions using shell scripts with compose run steps.
  - Encrypted secrets for an organization allows you to consolidate secrets across repositories.
  - Workflow templates for an organization streamlines and promotes best practices and consistency across your organization.

  GitHub Actions is not currently supported for enterprises using cluster configurations.

GitHub Packages

- GitHub Packages is a package hosting service, natively integrated with GitHub APIs, Actions, and webhooks. Create an end-to-end DevOps workflow that includes your code, continuous integration, and deployment solutions.

  Supported storage back ends include AWS S3 and MinIO with support for Azure blob coming in a future release. Please note that the current Docker support will be replaced by a beta of the new GitHub Container Registry in a future release. Please review the updated minimum requirements for your platform before you turn on GitHub

Packages.

When publishing packages to NuGet, users can now use the `--api-key` option to pass their authentication token instead of writing it into a file. For more information, see Configuring dotnet CLI for use with GitHub Packages

GitHub Packages is not currently supported for enterprises using cluster configurations.

GitHub Mobile beta

- GitHub Mobile beta allows you to triage notifications and manage issues and pull requests from your device. You can be simultaneously signed into mobile with one user account on GitHub.com and one user account on GitHub Enterprise Server.

  GitHub Mobile beta is now 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`.

Advanced Security Secret Scanning beta

- Secret Scanning beta scans public and private repositories for committed credentials, finds secrets, and notifies the secret provider or admin the moment they are committed into a repository.

  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.

Advanced Security Code Scanning

- GitHub Advanced Security code scanning is now generally available on GitHub Enterprise Server. Organizations who have purchased Advanced Security can use this capability to do static analysis security testing against their code, and prevent vulnerabilities from making it to their production code using CodeQL, our semantic analysis engine. For more information, see "Configuring code scanning on your appliance"

Changes

Administration Changes

- The webhook events delivery system has been rearchitected for higher throughput, faster deliveries, and fewer delayed messages. It also uses less CPU and memory in GitHub Enterprise Server 3.0+.
- Organization and Enterprise owners can now see when a team member has been promoted to or demoted from being a team maintainer in the audit log through the new `team.promote_maintainer` and `team.demote_maintainer` audit log events. For more information, see "Audited actions."
- Repository maintainers with existing GitHub Pages sites can easily update their prior default branch name.
- Additional hardware resources are required to run GitHub Enterprise Server with any of Actions, Packages or Advanced Security enabled. For more information on the minimum required resources for each supported platform, see "Setting up a GitHub Enterprise Server instance."
- Administrators can now publish a message, which all users must accept. This can help to onboard new users and surface other organization-specific information and policies.

Security Changes

- Organization owners can now disable publication of GitHub Pages sites from repositories in the organization.

Disabling GitHub Pages for the organization will prevent members from creating new Pages sites but will not unpublish existing sites. For more information, see "Disabling publication of GitHub Pages sites for your organization."

- A datacenter must be explicitly defined on all nodes before enabling an active replica.
- All usage of SSH fingerprints has been switched to use SHA256 fingerprints as they are used with OpenSSH since version 6.8 as well. This applies to the web interface and also the API where fingerprints are returned such as in GraphQL. The fingerprints follow the OpenSSH format.
- SHA-1 and SHA-256 signature headers (two headers) are sent on webhooks.

Developer Changes

- Majority of the services running in GitHub Enterprise Server 3.0+ are now on containers which internally enables GitHub to iterate fast and ship high quality releases
- The webhook events delivery system has been rearchitected for higher throughput, faster deliveries, and fewer delayed messages.

API Changes

- Administrators can now configure and manage the site-wide announcement banner via the REST API. For more information, see the endpoints for "GitHub Enterprise administration."
- A new API endpoint enables the exchange of a user to server token for a user to server token scoped to specific repositories. For more information, see "Apps" in the GitHub REST API documentation.

Default branch renaming

- Enterprise and organization administrators can now set the default branch name for new repositories. Enterprise administrators can also enforce their choice of default branch name across all organizations or allow individual organizations to choose their own.

  Existing repositories are unaffected by these settings, and their default branch name will not be changed.

  > The default branch for newly-created repositories will be set to `main` in GHES 3.1, unless you opt out by setting the default branch setting at the enterprise level.

  This change is one of many changes GitHub is making to support projects and maintainers that want to rename their default branch. To learn more about the changes we're making, see github/renaming.

Bug fixes

Fixes for known issues from Release Candidates

- All known issues from Release Candidate 1 and Release Candidate 2 have been fixed, except those listed in the Known Issues section below.

Fixes for other issues

- Issues with migrations and upgrades to 3.0.0 have been fixed.
- Backup Utilities versioning now works for release candidate versions.

- Generating a support bundle resulted in an error in the orchestrator logs.
- A large restore could result in Redis running out of memory.
- The checkbox to enable GitHub Actions in the Management Console is now visible with any authentication method.
- GitHub Actions could be enabled if the required storage was also configured.
- `ghe-repl-status` could silently fail if MSSQL replication was not configured.
- The format of several log files have changed, including the addition of a PID for different log types. This does not affect how GitHub Enterprise Support uses support bundles to troubleshoot issues.
- A PATCH request to the webhook configuration API no longer erases the webhook secret.
- Certain types of pre-receive hooks were failing.
- The Packages NuGet service now normalizes semantic versions on publish. An invalid semantic version (for example: v1.0.0.0.0.0) is not downloadable by NuGet clients and therefore a NuGet service is expected to normalize those versions (for example: v1.0.0.0.0.0 --> v1.0.0). Any original, non-normalized, version will be available in the `verbatimVersion` field. No changes to client configurations are required.

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 not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support.
- When GitHub Actions is enabled, use '`ghe-maintenance -u`' to unset maintenance mode.
- Duplicated logging to `/var/log/messages`, `/var/log/syslog`, and `/var/log/user.log` results in increased root volume utilization.
- Users can dismiss a mandatory message without checking all checkboxes.
- Pre-receive hook scripts cannot write temporary files, which may cause script execution to fail. Users who use pre-receive hooks should test in a staging environment to see if scripts require write access.
- Repository deploy keys are unable to be used with repositories containing LFS objects.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non-ASCII UTF-8 characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- Dependency graph fails to parse `setup.py` Python manifest files, resulting in HTTP 500 errors in logs. This, combined with the duplicated logging issue, results in increased root volume utilization.
- A race condition can cause dependency graph database migrations to appear to fail.
- Instances with a custom timezone that were upgraded from an earlier release of GitHub Enterprise Server may have incorrect timestamps in the web UI.
- Old builds of Pages are not cleaned up, which could fill up the user disk (`/data/user/`).

- When deleting a branch after merging a pull request, an error message appears although the branch deletion succeeds.
- 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.

Deprecations

Deprecation of GitHub Enterprise Server 2.19

- **GitHub Enterprise Server 2.19 is deprecated as of November 12, 2020**. 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 support for Semiotic

- The service supported a "Find by Symbol" experience in the pull request view that was not widely used.

Deprecation of workflow commands

- GitHub Actions `set-env` and `add-path` workflow commands have been deprecated. For more information, see the changelog.

Backups

- GitHub Enterprise Server 3.0 requires at least GitHub Enterprise Backup Utilities 3.0.0 for Backups and Disaster Recovery.