This version of GitHub Enterprise was discontinued on 2021-06-09. 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 2.21.23 **Download** **Print**

June, 10, 2021

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

- Import failures of organizations or repositories from non-GitHub sources could produce an `undefined method '[]' for nil:NilClass` error.

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

- 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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.22 **Download** **Print**

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

- An IP address added by an admin using the "Create Whitelist Entry" button could still be locked out.
- In a cluster or HA environment, GitHub Pages builds could be triggered on secondary nodes where they would fail.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.21 **Download** **Print**

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

- Packages have been updated to the latest security versions.

BUG FIXES

- 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.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.20 **Download** **Print**

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

- Setup script running on MySQL replication may have caused unnecessary database reseeding during database failover.
- `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.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.19 **Download** **Print**

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.

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- A warning message `jq: error (at <stdin>:0): Cannot index number with string "settings"` could occur during replica promotion.
- Visiting the `/settings/emails` page would store state that could cause improper redirects when logging out and logging back in.
- Dependency graph alerts weren't shown for some components whose advisories have upper case package names in `vulnerable_version_ranges`.
- User saw 500 error when executing git operations on an instance configured with LDAP authentication.
- When ghe-migrator encountered import errors, it would sometimes abort the entire process, and the logs did not include enough context.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.18 **Download** **Print**

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.

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

- Services were not transitioning to new log files as part of log rotation, resulting in increased disk usage.
- 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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.17 **Download** **Print**

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

- The `ghe-cluster-config-init` run was not fully accounting for the exit code of background jobs leading to improper handling of preflight checks.

CHANGES

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

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.16 **Download** **Print**

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.

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- Importing of repository archives from GitHub Enterprise Server that are missing repository files would fail with an 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 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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.15 **Download** **Print**

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.

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:** 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.
- **MEDIUM:** GitHub Tokens from GitHub Pages builds could end up in logs.
- **LOW:** A specially crafted request to the SVN bridge could trigger a long wait before failure resulting in Denial of Service (DoS).
- 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.
- 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.
- While restoring a large backup, exception logging related to Redis memory exhaustion could cause the restore to fail due to a full disk.

- 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.
- 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.
- When uploading a new license file with a different number of seats from the previous license file, the seat difference was not correctly represented in the enterprise account Settings -> License page.
- The "Prevent repository admins from changing anonymous Git read access" checkbox available in the enterprise account settings could not be successfully enabled or disabled.
- When a GitHub Pages build failed, the email notification contained an incorrect link for support location.
- During a leap year, the user was getting a 404 response when trying to view Contribution activity on a Monday.
- Visiting the *Explore* section failed with a 500 Internal Server error.

CHANGES

- Added support for AWS EC2 r5b instance types.
- Adjusted background queue prioritization to more evenly distribute jobs.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

December, 17, 2020

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

- **LOW:** High CPU usage could be triggered by a specially crafted request to the SVN bridge resulting in Denial of Service (DoS).
- Packages have been updated to the latest security versions.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.13 **Download** **Print**

December, 03, 2020

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

- Authorization service was being detected as unhealthy due to a race condition in the bootstrap which led to restart of the service.
- An underlying behavior was causing a service to become unavailable during the hotpatch upgrade process.
- A subset of log forwarding SSL certificates was not being applied correctly.

- Email notifications sent to suspended users when they were removed from a Team or an Organization.
- The way SSH certificates were applied between Organizations and Businesses was inconsistent.
- When an account was rate limited due to using incorrect passwords, it could be locked out for up to 24 hours.
- Pull request synchronization on repositories with many references could cause worker queues to fall behind.
- When signing in after attempting to visit a specific page, people were sent to the home page instead of their intended destination.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.12 **Download** **Print**

November, 17, 2020

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 babeld logs were missing a separator between seconds and microseconds.
- When the enterprise account "Repository visibility change" policy was set to "Enabled", organization owners could

not change the visibility of repositories within the organization.

- Audit logs could be attributed to 127.0.0.1 instead of the actual source IP address.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- 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.

Enterprise Server 2.21.11 **Download** **Print**

November, 03, 2020

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:** High CPU usage could be triggered by a specially crafted request to the SVN bridge resulting in Denial of Service (DoS).
- **LOW:** Incorrect token validation resulted in a reduced entropy for matching tokens during authentication. Analysis shows that in practice there's no significant security risk here.
- Packages have been updated to the latest security versions.

BUG FIXES

- Editing issues templates with filenames containing non-ASCII characters would fail with a "500 Internal Server Error".
- A metric gathering method for background jobs increased CPU utilization. (updated 2020-11-03)

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address.
- 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.

Enterprise Server 2.21.10 **Download** **Print**

October, 20, 2020

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 enterprise account "Confirm two-factor requirement policy" messaging was incorrect.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- 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.

Enterprise Server 2.21.9 **Download** **Print**

October, 09, 2020

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 user whose **LDAP** directory username standardizes to an existing GHES account login could authenticate into the existing account.
- Packages have been updated to the latest security versions.

BUG FIXES

- The NameID Format dropdown in the Management Console would be reset to "unspecified" after setting it to "persistent".
- Saving settings via the management console would append a newline to the TLS/SSL certificate and key files which triggered unnecessary reloading of some services.
- System logs for Dependency Graph were not rotating, allowing unbounded storage growth.
- Upgrade could fail if the resqued workers override setting is in use.
- When importing a repository with `ghe-migrator`, an unexpected exception could occur when inconsistent data is present.
- Links to GitHub Security Advisories would use a URL with the hostname of the GitHub Enterprise Server instance instead of GitHub.com, directing the user to a nonexistent URL.
- The enterprise account security settings page showed a "View your organizations' current configurations" link for the "Two-factor authentication" setting when the authentication mode in use does not support built in two-factor authentication.

- When using `ghe-migrator` to import PR review requests, records associated with deleted users would result in extraneous database records.
- When importing users with `ghe-migrator`, an error of "Emails is invalid" would occur if the system-generated email address were longer than 100 characters.
- Logging webhook activity could use large amounts of disk space and cause the root disk to become full.

CHANGES

- Support is added for the AWS EC2 instance type `m5.16xlarge`.
- Remove the requirement for SSH fingerprints in `ghe-migrator` archives as it can always be computed.
- GitHub App Manifests now include the `request_oauth_on_install` field.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- 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.

Enterprise Server 2.21.8 **Download** **Print**

September, 23, 2020

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**: ImageMagick has been updated to address DSA-4715-1.
- Packages have been updated to the latest security versions.

BUG FIXES

- Admins were unable to see delivered repository webhooks and instead saw "Sorry, something went wrong and we weren't able to fetch the deliveries for this hook".

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- 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.

Enterprise Server 2.21.7 **Download** **Print**

September, 08, 2020

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

- A service health check caused session growth resulting in filesystem inode exhaustion.
- Upgrading using a hotpatch could fail with an error: `'libdbi1' was not found`
- Configuring a repository's permission to `Triage` or `Maintain` no longer fails.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- 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.

Enterprise Server 2.21.6 **Download** **Print**

August, 26, 2020

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 was identified in GitHub Pages 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 affected all versions of GitHub Enterprise Server. The underlying issues contributing to this vulnerability were identified both internally and through the GitHub Security Bug Bounty program. We have issued CVE-2020-10518.
- **MEDIUM:** An improper access control vulnerability was identified that allowed authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and has been assigned CVE-2020-10517. The vulnerability was reported via the GitHub Bug Bounty program.
- Packages have been updated to the latest security versions.

BUG FIXES

- A message was not logged when the ghe-config-apply process had finished running ghe-es-auto-expand.
- Excessive logging to the `syslog` file could occur on high-availability replicas if the primary appliance is unavailable.
- Database re-seeding on a replica could fail with an error: `Got packet bigger than 'max_allowed_packet'`
- In some cases duplicate user data could cause a 500 error while running the ghe-license-usage script.
- Using `ghe-migrator`, the `add` command would fail to lock a repository when using the `--lock` flag.

CHANGES

- In a high availability or geo-replication configuration, replica instances would exit maintenance mode when ghe-config-apply ran.
- We've added support for the R5a and R5n AWS instance types.
- Removed the license seat count information on the administrative SSH MOTD due to a performance issue impacting GitHub Enterprise Server 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 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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.5 **Download** **Print**

August, 12, 2020

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

- Resolved an issue that could lead to high CPU usage while generating system configuration templates.
- Recent changes to memory allocations could lead to a degradation in system performance
- Temporary connectivity issues while running database migrations could cause data loss.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.4 **Download** **Print**

August, 11, 2020

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 was identified in GitHub Pages that could allow an attacker to execute commands as part building a GitHub Pages site. This issue was due to an outdated and vulnerable dependency used in the Pages build process. 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. To mitigate this vulnerability, Kramdown has been updated to address CVE-2020-14001.
- **HIGH:** High: An attacker could inject a malicious argument into a Git sub-command when executed on GitHub

Enterprise Server. This could allow an attacker to overwrite arbitrary files with partially user-controlled content and potentially execute arbitrary commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to access repositories within the GHES instance. However, due to other protections in place, we could not identify a way to actively exploit this vulnerability. This vulnerability was reported through the GitHub Security Bug Bounty program.

- Packages have been updated to the latest security versions.

BUG FIXES

- A Consul configuration error prevented some background jobs from being processed on standalone instances.
- The service memory allocation calculation could allocate an incorrect or unbounded memory allocation to a service resulting in poor system performance.
- The virtualization platform for oVirt KVM systems was not properly detected, causing problems during upgrades.
- The error message for invalid authentication with a password via Git command line didn't populate the URL linking to adding the appropriate token or SSH key.
- Creating an issue on a user repository using the Issue Template feature could fail with an Internal Server Error.
- Visiting the *Explore* section failed with a 500 Internal Server error.
- Issues could not be sorted by *Recently updated* on repositories migrated to a new instance.
- GitHub Connect was using a deprecated GitHub.com API endpoint.
- Internal metrics gathering for background jobs contributed to CPU and memory use unnecessarily.
- The 404 page contained GitHub.com contact and status links in the footer.
- Background jobs for an unreleased feature were queued and left unprocessed.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.3 **Download** **Print**

July, 21, 2020

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 Management Console monitor graphs would sometimes not display correctly on larger screens.
- GitHub App Manifest creation flow was unusable in some scenarios when a SameSite Cookie policy was applied.
- In some circumstances, accessing the 'Explore' page would throw an application 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 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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.2 **Download** **Print**

July, 09, 2020

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

SECURITY FIXES

- **MEDIUM:** Updated nginx to 1.16.1 and addressed CVE-2019-20372. (updated 2020-07-22)
- Packages have been updated to the latest security versions.

BUG FIXES

- Certain log files did not rotate every 7 days.
- Rapid reuse of webhook source ports resulted in rejected connections.
- Incorrect background jobs could attempt to run on instances configured as passive replicas.
- The VPN between nodes could become unstable causing errors to be logged and free space on the root volume to be exhausted.
- Internal repositories were not correctly included in search results for SAML-enabled orgs.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.1 **Download** **Print**

June, 23, 2020

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

- Excessively large log events could lead to log forwarding instability when UDP was used as the transport mechanism.
- The internal communication service used to access MySQL could restart more often than required, including part way through the upgrade process, which could cause the upgrade to partially fail. We have reduced the rate of restarts and made the code more robust.
- Automatic unsuspension of a user through SSO did not complete if the SSH keys attribute had keys already associated with the user's account.
- The repository permission hash from the REST API indicated no access for business members who have pull access to internal repositories.
- The "Repository issue deletion" Enterprise account policy did not reflect the currently saved setting.
- The audit log did not include branch protection changes events.

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.
- Security alerts are not reported when pushing to a repository on the command line.
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

Enterprise Server 2.21.0 **Download** **Print**

June, 09, 2020

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.

FEATURES

- Users can manage notifications on issues, pull requests and other subjects when navigating from a web notification.
- Users can convert a pull request back to a "Draft".
- Multi-line suggestions let a user suggest a specific change to multiple lines of code when reviewing a pull request.
- Users with write access to a repository can hide a comment in an issue or pull request as a "Duplicate" .
- When creating a repository from a template a user can optionally select to include all branches, rather than just the default branch.
- Issue project cards include a linked pull requests section so a user can see what development work is related to the issue directly from the project board.
- There are a new set of "Deleting reactions" endpoints in the Reactions API. The existing "Delete reactions" endpoints will be deprecated in early 2021.
- There are a new set of Teams API endpoints which will allow GitHub to scale and support the Teams API long-term. The existing API endpoints will be deprecated in early 2021.
- Users can create links between issues and pull requests without needing to use closing keywords in the pull request description.

SECURITY FIXES

- An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21. We have issued CVE-2020-10516 in response to this issue. The vulnerability was reported via the GitHub Bug Bounty program.

BUG FIXES

- If a user with push access minimized another user's comment, the author of the comment could unminimize it even if they had insufficient privileges.
- Users could accidentally merge to master from the issue template editor and blob editor.

- When a user deleted an account from GitHub, the audit log records did not correctly show organization removal records.
- The gist avatar for the current user would link to a non-existent URL.
- The organization repositories tab count did not include internal repositories.
- Clicking the "Show All Teams" button when transferring a repository caused a 500 error.
- Long filenames could cause overflow issues when showing the 'Changed since last view' label or the 'Show rich' diff toggle on the diff file view.
- Hovercards for organization teams misreported their member size.
- The pull request review comment popup window had a scrolling issue.
- Haproxy could become saturated causing a slowdown in git operations.
- The Dependency Graph feature was not automatically enabled after HA replica promotion.
- A timeout could be triggered on the releases index page for repositories with thousands of draft pull requests.
- It was not possible to filter pull requests by both state and draft at the same time.
- If a pull request changed a submodule pointer, then clicking "Edit file" on that submodule file from the "Files changed" tab of the pull request page caused a 404 error.
- It was not possible to add users to an organization, or delete the organization, following the bulk removal of all users and admins from that organization.
- Review comments against files containing diacritics and non-Latin characters in the filename on the "Files changed" page would disappear when the page is reloaded.
- The state of the "Viewed" checkbox was not retained for files containing diacritics and non-Latin characters in the filename on the "Files changed" page.
- Pull requests showed the "Approved" badge when not all required reviews were in place.
- The tag dropdown was empty when searching for a tag in repositories with more than 100 tags.
- Pull request pages showing annotations with non UTF-8 titles could encounter encoding errors in view rendering.
- A race condition for refresh on the OAuth page could cause a redirect to be executed twice.
- The "Personal Access Tokens" page would timeout if there are more than 10 tokens.
- Scheduled LDAP User and Team Sync jobs could be started while previously scheduled Sync jobs were still in process. A locking mechanism has been implemented to prevent new Sync jobs from starting if one is still running.

CHANGES

- The web notifications interface, including new states , filters and shortcuts have been updated.
- It is now possible to disable reactivation of LDAP users on LDAP sync.
- The push protected branch wording has been updated to clarify that admins can always push and that users with the Maintain role can push when status checks pass.
- Prevent blank commit when suggestion is identical to original text.
- Pagination is supported as a way to get more files in the diff associated with a commit via the REST API.
- Admins can enable, disable, delete, and search for webhooks using the webhook ID from the command line using `ghe-webhook-manage`.

- Automatic base retargeting will happen after manual head reference cleanup for a merged pull request.
- SVG files are handled as text and as images in the diff viewer.
- The "auto delete branches on merge" setting can be set when creating and updating repositories using the REST API.
- A new endpoint has been added to delete a deployment through the REST API.
- Admins can enable security alerts but disable all notifications from those alerts.
- The Pages log shows the user login accessing the GitHub Pages site.
- Enterprise members can see all of the organizations they belong to as part of their Enterprise account from one view by navigating to `https://[ghes-hostname]/enterprises/[account-name]`.
- REST API support for triage and maintain roles has been expanded.
- A user can create and share search queries that resolve to the current user by using the `@me` search syntax.
- New issue template configuration options have been added.
- MySQL backup and restore reliability and time to completion has been improved.
- Improved visibility of pull requests and issue references in the issue sidebar, issue cards and issue list.
- Users can filter and search by `linked:pr` or `linked:issue`.
- Automatic failover of MySQL within a single region for Cluster deployments is now possible.
- A user can compare tags between two releases to determine what changes have been made on the releases page.
- Outdated comments are no longer collapsed by default on the Pull Request timeline. They can be collapsed by resolving the thread.
- Admins can view a list of logins reserved for internal use by navigating to the "Reserved logins" stafftools tab.

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 pushing to a gist, an exception could be triggered during the post-receive hook.
- 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.
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Audit logs may be attributed to 127.0.0.1 instead of the actual source IP address. (updated 2020-11-02)
- Configuring a repository's permission to `Triage` or `Maintain` fails with an error message.
- 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.

© 2021 GitHub, Inc. Terms Privacy Security Status Help Contact GitHub Pricing Developer API Training About