This version of GitHub Enterprise was discontinued on 2021-03-02. 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.

2.20 Release notes

2.21 ›

Enterprise Server 2.20.24

Download **Print**

March 01, 2021

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.
- **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

- 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 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.

- During a leap year, the user was getting a 404 response when trying to view Contribution activity on a Monday.

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.

Enterprise Server 2.20.23 Download Print

December 16, 2020

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.

Enterprise Server 2.20.22 **Download** **Print**

December 02, 2020

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.

Enterprise Server 2.20.21 Download Print

November 16, 2020

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.

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.

Enterprise Server 2.20.20 Download Print

November 02, 2020

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

- Suspended users were included in the list of suggested users, potentially hiding unsuspended users.

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.

Enterprise Server 2.20.19 Download Print

October 19, 2020

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.

Enterprise Server 2.20.18 Download Print

October 08, 2020

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.
- 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.
- When importing a repository with `ghe-migrator`, an unexpected exception could occur when inconsistent data is present.
- 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.

Enterprise Server 2.20.17 Download Print

September 22, 2020

SECURITY FIXES

- **MEDIUM**: ImageMagick has been updated to address DSA-4715-1.
- 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.

Enterprise Server 2.20.16 Download Print

September 07, 2020

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`

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.

Enterprise Server 2.20.15 Download Print

August 25, 2020

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.

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.

Enterprise Server 2.20.14

Download Print

August 11, 2020

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

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.

Enterprise Server 2.20.13

Download Print

August 10, 2020

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:** 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 GitHub Enterprise Server 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.
- GitHub Connect was using a deprecated GitHub.com API endpoint.
- Issues could not be sorted by *Recently updated* on repositories migrated to a new instance.
- The 404 page contained GitHub.com contact and status links in the footer.

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.

Enterprise Server 2.20.12 Download Print

July 20, 2020

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.

CHANGES

- Improvements to HAProxy scaling.

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.

Enterprise Server 2.20.11 Download Print

July 08, 2020

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

- Dependency graph was not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes.
- 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.

- 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.

Enterprise Server 2.20.10 Download Print

June 22, 2020

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.
- 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.
- Previewing a GitHub App description written in markdown was not properly rendered.
- The audit log did not include branch protection changes events.
- Trying to assign code review to a member of an empty team would result in a '500 Internal Server Error'.
- Code review assignment using the load balancing algorithm could repeatedly assign to the same team member.

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.
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.9 Download Print

June 01, 2020

SECURITY FIXES

- **HIGH:** 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.
- Packages have been updated to the latest security versions.

BUG FIXES

- Internet-facing GitHub Enterprise Server instances could be indexed by search engines.

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)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.8 Download Print

May 18, 2020

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- After the license file was updated, services were not properly reloaded causing functionality loss.
- Internal API requests updating Dependency Graph information could fail if the response body was too large.
- The `affiliations` argument to some GraphQL repository connections was not respected.
- Automatic unsuspension of a user through SSO did not complete if the SAML email attribute had different casing than the GitHub user email.
- Restoring the membership of a user to an organization did not instrument the actor in webhook and audit log payloads.

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)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.7 Download Print

May 04, 2020

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- `ghe-repl-start` and `ghe-repl-status` displayed syntax errors.
- If a repository has the "automatically delete head branches" setting enabled, the head branch wasn't automatically deleted, when a pull request was merged by a GitHub App installation.
- When an organization member was reinstated, the webhook payload reported the `ghost` user as the sender and not the actual user performing the reinstatement.
- If a repository has the "automatically delete head branches" setting enabled, the head branch wasn't automatically deleted where the head repository was different from the base repository.
- The garbage collection of temporary files could lead to a license validation error.
- In some situations, including when a repository is first created, the pre-receive hook would be run without a value populated for the GITHUB_REPO_PUBLIC environment variable.

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)

- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.6 Download Print

April 22, 2020

SECURITY FIXES

- **HIGH**: OpenSSL has been updated to address CVE-2020-1967.
- **HIGH**: Git has been updated to address CVE-2020-5260 and CVE-2020-11008. New restrictions prevent malicious repositories from being pushed to the server instance, protecting clients which have not yet been patched.
- **LOW**: ImageMagick has been updated to address CVE-2019-10131.
- Packages have been updated to the latest security versions.

BUG FIXES

- The git user lacked permissions to invoke the processes required to convert existing repositories using Subversion, from the v4 format to v3 LRS.
- A mismatch in MySQL configurations could cause backups to fail in large installations.
- When upgrading from previous versions, background job workers would sometimes not spawn, preventing essential features such as merging pull requests.
- When a GitHub Enterprise Server license contained non-ASCII characters, a `GET` request to the Management Console's API `/setup/api/settings` endpoint would result in an Internal Server Error.
- The recovery console would prompt for a root password, even if the root account was locked.
- A CODEOWNERS file with a leading UTF-8 Byte Order Mark would cause all codeowner rules to be ignored.

CHANGES

- When the orchestrator-client cron job failed, multiple emails would be sent to the root account.
- When an external identity provider controlled user's site administrator status, users could not be demoted via the command line utility.

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)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.5 **Download** **Print**

April 06, 2020

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- A maximum Git object size of 100MB option could not be selected for a repository when the global enterprise account had a Git object size option other than 100MB set.
- Results from the the Issues and Pull Requests API could have inconsistent behaviour when ordering by the `updated_at` field.
- The SecurityVulnerability `package` field could not be queried via the GraphQL API.
- Changing a repository from *public* to *internal* displayed an irrelevant billing message.

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.
- When upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests.
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.4 Download Print

March 24, 2020

BUG FIXES

- SAML Authentication requests and Metadata were not strictly encoded, causing some Identity Providers to not correctly process Service Provider initiated Authentication requests.
- `ghe-migrator` exports did not contain milestone users, which could break import operations.
- When pushing to a Gist, an exception could be triggered during the post-receive hook.
- `ghe-repl-status` could fail when trying to display repositories that were not fully replicated.

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.
- When upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests. (updated 2020-04-07)
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.3 Download Print

March 11, 2020

BUG FIXES

- Upgrades and settings updates would fail if background worker configurations had been customised.

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.
- When upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests. (updated 2020-04-07)
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.2 Download Print

March 09, 2020

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- In some cases the forwarded log entries, mainly for audit.log were getting truncated.
- The `ghe-license-check` command-line utility returned an "Invalid license file" error for some valid licenses, causing configuration changes to fail.
- Alambic exception logs were not forwarded by syslog.
- The `org_block event` is not unavailable but was appearing for GitHub Apps on GitHub Enterprise Server.
- GraphQL query responses sometimes returned unmatched node identifiers for `ProtectedBranch` objects.
- The GitHub App credential used by GitHub Connect failed to refresh immediately after expiry.
- Leaving a comment in reply to a pull request comment was intermittently creating a pending pull request review.
- Using ghe-migrator or exporting from GitHub.com, an export would silently fail to export non-image attachments.
- Pre-receive hook returned 500 error on web UI when UTF-8 characters were encountered.

CHANGES

- The `ghe-license-usage` command-line utility includes a new `--unencrypted` option to provide visibility into the exported license usage file.

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.
- Upgrades and settings updates will fail if background worker configurations have been customised.
- 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 upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests. (updated 2020-04-07)
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.1 Download Print

February 26, 2020

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- Restore from backups would fail with an `Invalid RDB version number` error.
- Upgrading an HA replica would stall indefinitely waiting for MySQL to start.
- PR review comments with unexpected values for "position" or "original_position" caused imports to fail.
- Duplicate webhook entries in the database could cause upgrades from previous versions to 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 pushing to a gist, an exception could be triggered during the post-receive hook.
- Upgrades and settings updates will fail if background worker configurations have been customised.
- 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 upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests. (updated 2020-04-07)
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)

Enterprise Server 2.20.0 Download Print

February 10, 2020

FEATURES

- On a repository branch, repository administrators can reject any push that contains a merge commit by enabling `Require linear history` using branch protection rules.
- Repository administrators can grant all users with push access the ability to force-push to a protected branch by enabling `Allow force pushes` using branch protection rules.
- Repository administrators can grant all users with push access the ability to delete a protected branch by enabling `Allow deletions` using branch protection rules.
- Administrators can set a `maxobjectsize` limit on repositories, limiting the size of push commits to a repository that are not in Git LFS.
- Organization owners can create a set of default labels when creating a new repository.

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- When a member of an organization tried to view a public repository in that organization, an SSO prompt could break the page display.
- When viewing a users' profile, the links to that users' teams could be broken.
- Users with the `maintain` role were unable to edit repository topics.
- A user who isn't an administrator for an organization would receive a 500 error when attempting to access the sign up page.
- The edit history popup would not display on gist comments.
- A new account could be registered with an email that was already registered.
- A storage service was hitting a file descriptor limit and causing kernel hanging and other services to log errors.
- When an autolink reference was part of a url, the hyperlink could be removed.
- When adding a comment to a pull request, the `Linked Issues` section from the sidebar could disappear.
- When editing an existing organization invitation for a user, a duplicate header could be appear on the `Teams` table.
- The `resqued` service could stop logging events when the queues became too large.
- Self-signed certificates are not automatically generated when running the `ghe-config-apply` command for cluster and high-availability configurations.

CHANGES

- No logo will be displayed for a topic if one has not been uploaded.

- When viewing an issue on a mobile browser, the issue metadata is listed at the top of the page.
- Consul's top-level domain has changed from ".consul" to ".ghe.local".
- The hookshot service no longer relies on ElasticSearch and only uses MySQL as a database store.
- Improved visual distinction between issue, project and discussion has been implemented on project note cards.
- On a pull request review, a notice is displayed if a multi-line comment is truncated.
- Users can view their audit log on the `Security Log` tab of their personal 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 pushing to a gist, an exception could be triggered during the post-receive hook.
- Duplicate webhook entries in the database can cause upgrades from previous versions to fail. (updated 2020-02-26)
- Upgrades and settings updates will fail if background worker configurations have been customised.
- 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 upgrading from previous versions, background job workers may not be spawned, preventing essential features such as merging pull requests. (updated 2020-04-07)
- Security alerts are not reported when pushing to a repository on the command line. (updated 2020-06-23)
- Dependency graph is not detecting dependencies when deployed in a cluster configuration with multiple Redis nodes. (updated 2020-06-30)