This version of GitHub Enterprise was discontinued on 2021-09-23. 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.

‹ 2.21

Enterprise Server 2.22 release notes

3.0 ›

Enterprise Server 2.22.22 **Download**

September, 24, 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

- **HIGH:** A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This is the result of an incomplete fix for CVE-2021-22867. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned CVE-2021-22868.

BUG FIXES

- The GitHub Connect configuration of the source instance was always restored to new instances even when the `--config` option for `ghe-restore` was not used. This would lead to a conflict with the GitHub Connect connection and license synchronization if both the source and destination instances were online at the same time.
- Fixes GitHub Pages builds so they take into account the NO_PROXY setting of the appliance. This is relevant to appliances configured with an HTTP proxy only.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.21 Download

September, 07, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.20 Download

August, 24, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- Journald messages related to automatic updates (`Adding h/m/s random time.`) were logged to syslog.
- Git hooks to the internal API that result in failing requests returned the exception `undefined method body for "success":String (NoMethodError)` instead of returning an explicit `nil`.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.19 Download

August, 10, 2021

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

BUG FIXES

- Audit log entries for changes made to "Repository creation" organization settings were inaccurate.

CHANGES

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

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.18 Download

July, 27, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- A significant number of 503 errors were being created if the scheduled job to sync vulnerabilities with GitHub.com attempted to run when dependency graph was not enabled and content analysis was enabled.
- Unauthenticated HTTP proxy for the pages containers build was not supported for any users that use HTTP proxies.

CHANGES

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

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.17 Download

July, 14, 2021

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

SECURITY FIXES

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

BUG FIXES

- `ghe-cluster-config-node-init` would fail during cluster setup if HTTP proxy is enabled.
- Collectd would not resolve the forwarding destination hostname after the initial startup.
- The job that purged stale deleted repositories could fail to make progress if some of those repositories were protected from deletion by legal holds.
- Git pushes could result in a 500 Internal Server Error during the user reconciliation process on instances using LDAP authentication mode.
- A significant number of 503 errors were logged every time a user visited a repository's `/settings` page if the dependency graph was not enabled.

CHANGES

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

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.16 Download

June, 24, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- The sshd service would sometimes fail to start on instances running on Google Cloud Platform.
- Old upgrade files would persist on the user disk, sometimes resulting in out of space conditions.
- An export archive would silently fail to import pull requests if they contained review requests from teams not present in the archive.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.15 Download

June, 10, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- Import failures of organizations or repositories from non-GitHub sources could produce an `undefined method '[]' for nil:NilClass` error.
- GitHub profile names might have changed unintentionally when using SAML authentication, if the GitHub profile name did not match the value of the attribute mapped to the `Full name` field in the Management Console.

CHANGES

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

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are removed during the upgrade process.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository, where the blob's file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.14 Download

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

- Normal replication delays in MSSQL generated warnings.
- An IP address added by an admin using the "Create Whitelist Entry" button could still be locked out.
- `spokesd` created excessive log entries including the phrase "fixing placement skipped".

CHANGES

- Check annotations older than 4 months will be archived.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.13 Download

May, 13, 2021

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

SECURITY FIXES

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

BUG FIXES

- Orchestrator auto failover could be enabled during the phase of config apply.
- Users with maintainer permissions to a repository were shown an e-mail verification warning instead of a successful

page build on the repository Pages settings page.

- The code owner of a wildcard rule would be incorrectly added to the list of owners for the code owners badge even if a later rule took precedence for that path.
- OpenAPI documentation referred to an invalid header.

CHANGES

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

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.12 Download

April, 28, 2021

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

SECURITY FIXES

- Packages have been updated to the latest security versions.

BUG FIXES

- During upgrades, the process would pause indefinitely after `cleanup nomad job`.
- Failing `ghe-cluster-failover` with the error message `Trilogy::Error: trilogy_connect`.
- `ghe-cluster-status-mysql` showed warnings about failovers as errors.
- Setup script running on MySQL replication may have caused unnecessary database reseeding during database failover.
- `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.
- Customers with more than three storage hosts were unable to restore to their disaster-recovery cluster due to the fullest disks being selected instead of empty nodes.

CHANGES

- Preflight checks allow all AWS instance types by default.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.11 Download

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.
- Continuously restoring backups to a cluster could fail due to MySQL replicas failing to connect to the primary.
- Syntax highlighting could fail due to the Treelights container running out of memory.
- 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`.
- GitHub integration apps were not able to notify teams when mentioned directly via an at-mention in an issue comment.
- 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.
- 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 2.22.10 Download

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

- A timezone set on GitHub Enterprise 11.10.x or earlier was not being used by some services which were defaulting to UTC time.
- Services were not transitioning to new log files as part of log rotation, resulting in increased disk usage.
- The 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.
- 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 2.22.9 Download

March, 23, 2021

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

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

SECURITY FIXES

- **HIGH:** A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to override environment variables leading to code execution on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.3 and was fixed in 3.0.3, 2.22.9, and 2.21.17. This vulnerability was reported via the GitHub Bug Bounty program and has been assigned CVE-2021-22864.
- Packages have been updated to the latest security versions.

BUG FIXES

- Running `ghe-cluster-config-init` could cause a cluster to become inoperable.
- Systemd could lose track of HAProxy's PID.
- The mysql-failover warning was displayed indefinitely after a successful failover.
- The `ghe-cluster-config-init` run was not fully accounting for the exit code of background jobs leading to improper handling of preflight checks.
- A Security & Analysis link did not appear in the left-side navigation on the Settings page for repositories.
- After disabling GitHub Packages, some organization pages would return an HTTP 500 error response.

CHANGES

- Improves reliability of nomad services by implementing the same restart policy introduced in GitHub Enterprise Server 3.0.
- Use a relative number for consul and nomad `bootstrap_expect` allowing for a cluster to bootstrap even if a handful of nodes are down.
- Logs will rotate based on size in addition to time.
- Added kafka-lite to the `ghe-cluster-status` command.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.

- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- 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 2.22.8 Download

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

- Systemd journal logs were duplicated in multiple places.
- A site admin could get a 500 error page while trying to view issues referenced from private repositories.
- 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.
- Users may experience assets such as avatars not loading, or a failure to push/pull code. This may be caused by a PID mismatch in the `haproxy-cluster-proxy` service. To determine if you have an affected instance:

  Single instance

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

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

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

  Cluster or High Availability configuration

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

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

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

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

Enterprise Server 2.22.7 Download

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 first setting up a new instance, if you selected "Configure as Replica" you would be unable to start replication.

- When GitHub Actions was enabled, disabling maintenance mode in the management console failed.

- 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.

- User saw 500 error when executing git operations on an instance configured with LDAP authentication.

- The `remove_org_member_package_access` background job was visible in the management console and would continually increase.

- 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.

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.
- Users may experience assets such as avatars not loading, or a failure to push/pull code. This may be caused by a PID mismatch in the `haproxy-cluster-proxy` service. To determine if you have an affected instance:

  Single instance

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

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

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

  Cluster or High Availability configuration

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

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

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

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

Enterprise Server 2.22.6 Download

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.

BUG FIXES

- Requests for some file resources like a zip archive or raw file could enter a redirection loop.
- A timeout could prevent some Issues and Pull Requests searches from providing complete search results.
- Custom tabs with non-alphabetic characters in small screens did not render correctly.
- An underlying behavior was causing failures when pushing content to a Git LFS-enabled repository.
- In some rare cases issues could cause a 500 error when accessed via the web interface.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.5 Download

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.
- The Elasticsearch upgrade process was not getting captured by ghe-diagnostics.
- Enabling GitHub Actions on an upgraded high availability configuration caused errors in replication.
- An underlying behavior was causing a service to become unavailable during the hotpatch upgrade process.
- Users connecting to an active replica would get an error connecting to the live updates websocket.
- 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 with a local username and password (built-in authentication) after attempting to visit a specific page, the user was sent to the home page instead of their intended destination.
- For GHES instances using built-in authentication with an internal SAML identity provider, users without an associated email address could not create a commit from the web interface.

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When a replica node is offline in a high availability configuration, GitHub Enterprise Server may still route GitHub Pages requests to the offline node, reducing the availability of GitHub Pages for users.

Enterprise Server 2.22.4 Download

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.
- After upgrading GHES with a hotpatch, the `ghe-actions-precheck` and `ghe-packages-precheck` commands would fail with the error `"docker load" accepts no arguments`.
- 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.
- 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 2.22.3 Download

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

- **LOW:** High CPU usage could be triggered by a specially crafted request to the SVN bridge resulting in Denial of Service (DoS) on the SVN bridge service. (updated 2020-11-16)
- **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

- GitHub Actions could fail to start up successfully if it was previously enabled on an instance running 2.22.0 and was upgraded to 2.22.1 or 2.22.2.
- Configuration files for GitHub Actions were not copied to the replica when setting up high availability replicas potentially leading to errors during `ghe-repl-promote`.
- On a freshly set up 2.22.1 or 2.22.2 instance or after upgrading to 2.22.1 or 2.22.2, the activity feed on an organization's dashboard would not update.
- 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.
- 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 2.22.2 Download

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

- If the storage account settings failed to validate while configuring GitHub Actions, running `ghe-actions-teardown` was required before making a new attempt.
- A custom proxy configuration could adversely affect the GitHub Actions environment.
- On a change of an address on eth0, Nomad and Consul could get unresponsive.
- When using self-signed certificates, GHES could have SSL validation exceptions upon configuring GitHub Actions.
- Using a GitHub Action from a branch name with a `+` or `/` character resulted in an error: `Unable to resolve action`.
- The enterprise account "Confirm two-factor requirement policy" messaging was incorrect.
- On certain requests above 100MB, Kafka's buffer could be over-allocated.

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.
- GitHub Actions can fail to start up successfully if it was previously enabled on an instance running 2.22.0 and is upgraded to 2.22.2. (updated 2020-10-23)
- On a freshly set up 2.22.2 instance or after upgrading to 2.22.2, the activity feed on an organization's dashboard will no longer update. (updated 2020-10-27)
- 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 2.22.1 Download

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

- **MEDIUM**: ImageMagick has been updated to address DSA-4715-1.
- Requests from a GitHub App integration to refresh an OAuth access token would be accepted if sent with a different, valid OAuth client ID and client secret than was used to create the refresh token.
- 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".
- Upgrading using a hotpatch could fail with an error: `'libdbi1' was not found`
- 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.
- The MS SQL Server performance graph showed statistics from the primary instance even when a replica was selected.
- `ghe-actions-precheck` would silently exit without running the storage checks if Actions was not enabled.
- Upgrade could fail if the resqued workers override setting is in use.
- Some services running in containers were not sending logs to the journal.
- 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.
- 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.
- OAuth refresh tokens would be removed prematurely.
- Search repair tasks would generate exceptions during the migration phase of configuration.

- On the settings page for GitHub Apps, the "Beta Features" tab was not visible in some circumstances.
- 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.
- Users experienced slower Git clone and fetch performance on an instance with high availability replicas due to reads being forwarded to a different node.
- The repository Settings page of a repository for a user or organization GitHub Pages sites would fail with a "500 Internal Server Error".
- Repository network maintenance operations could become stuck in a `running` state.
- A repository being deleted immediately after uploading a code scanning result could cause a stall in the processing of code scanning results for all repositories.
- When a large number of code scanning results were submitted at the same time, processing of batches could time out resulting in a stall in processing of code scanning results.
- Creating a GitHub App from a manifest would fail.
- GitHub usernames were changed unintentionally when using SAML authentication, when the GitHub username did not match the value of the attribute mapped to the `username` field in the Management Console.

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.
- Configuration updates will fail when restoring data to a GitHub Actions-enabled instance if the original backup source did not have the feature enabled.
- GitHub Actions can fail to start up successfully if it was previously enabled on an instance running 2.22.0 and is upgraded to 2.22.1. (updated 2020-10-23)
- On a freshly set up 2.22.1 instance or after upgrading to 2.22.1, the activity feed on an organization's dashboard will no longer update. (updated 2020-10-27)

- 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 2.22.0 Download

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.

GitHub is excited to present GitHub Enterprise Server 2.22.0.

FEATURES

GITHUB ACTIONS BETA

- GitHub Actions is a powerful, flexible solution for CI/CD and workflow automation. GitHub Actions on Enterprise Server includes tools to help you manage the service, including key metrics in the Management Console, audit logs and access controls to help you control the roll out.

  You will need to provide your own storage and runners for GitHub Actions. AWS S3, Azure Blob Storage and MinIO are supported. Please review the updated minimum requirements for your platform before you turn on GitHub Actions. To learn more, contact the GitHub Sales team or sign up for the beta.

GITHUB PACKAGES BETA

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

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

ADVANCED SECURITY CODE SCANNING BETA

- GitHub Advanced Security code scanning is a developer-first, GitHub-native static application security testing (SAST). Easily find security vulnerabilities before they reach production, all powered by the world’s most powerful code analysis engine: CodeQL.

  Administrators using GitHub Advanced Security can sign up for and enable GitHub Advanced Security code scanning beta. Please review the updated minimum requirements for your platform before you turn on GitHub Advanced Security code scanning.

PULL REQUEST RETARGETING

- When a pull request's head branch is merged and deleted, all other open pull requests in the same repository that target this branch are now retargeted to the merged pull request's base branch. Previously these pull requests were closed.

SUSPEND AND UNSUSPEND AN APP INSTALLATION

- Administrators and users can suspend any GitHub App’s access for as long as needed, and unsuspend the app on command through Settings and the API. Suspended apps cannot access the GitHub API or webhook events. You can use this instead of uninstalling an application, which deauthorises every user. ''

IMPROVED LARGE SCALE PERFORMANCE

- We have revised the approach we take to scheduling network maintenance for repositories, ensuring large monorepos are able to avoid failure states. ''

  Passive replicas are now supported and configurable on GitHub Enterprise Server cluster deployments. These changes will enable faster failover, reducing RTO and RPO.

VIEW ALL OF YOUR USERS

- For exceptionally large teams, administrators can adjust the 1,500 default maximum for user lists. ''

CHANGES

ADMINISTRATION CHANGES

- Shared workers have been enabled to make live updates more resilient by sharing connections across tabs.
- The "Contact Support" link on `50x` error pages now links to the support email or link configured in the Management Console.
- It's now possible to manage global announcements and expiration dates through the enterprise account settings.
- You can now exempt certain users from the default API rate limits configured in the management console, if necessary.
- Repository administrators can now set their repository to any available visibility option from a single dialog in the repository's settings. Previously, you had to navigate separate sections, buttons, and dialog boxes for changing between public and private and between private and internal.
- A new Enterprise settings link on the user dropdown menu makes it easier to navigate to Enterprise Account Settings.
- The legacy "Admin Center" link on the /stafftools page has been removed. The "Enterprise" link is now the best way to navigate to the Enterprise Account from the /stafftools page.
- The Options sub-menu item in the Enterprise Account settings has been moved from the Settings section to the Policies section.
- Accessing resources by using a personal access token or SSH key now counts as user activity. This relieves administrators from the burden of filtering out certain users from the user dormancy reports and makes it safer to use the "Suspend all" button without accidentally suspending users who only accessed GitHub in a read-only way over the APIs with a Personal Access Token (PAT) or SSH key.

SECURITY CHANGES

- Two-factor recovery codes can no longer be used during the two-factor sign in process. One-Time-Passwords are the only acceptable values.
- When a user is signed into GitHub Enterprise Server through single sign-on, the default repository visibility

selection is Private.

- Owners of GitHub Apps can now choose to have their user-to-server access tokens expire after 8 hours, to help enforce regular token rotation and reduce the impact of a compromised token.

DEVELOPER CHANGES

- The GitHub UI has undergone a design refresh, and the repositories homepage has been redesigned, including a responsive layout and improved mobile web experience.
- In the "Clone with SSH" repository dropdown menu, users will now be notified if they do not have any keys setup.
- Commits are now ordered chronologically in the pull request timeline and commits tab. This new ordering is also reflected in the "List commits on a pull request" REST API and GraphQL "PullRequest object" timeline connection.
- Users can now set a skin tone default for emoji autocomplete results in comment text areas.
- Tree-sitter improves syntax highlighting and is now the default library used for language parsing.

USERS AND ORGANIZATIONS CAN ADD TWITTER USERNAMES TO THEIR GITHUB PROFILES

- Developers and organizations can now add their Twitter username to their profile

API CHANGES

- **Graduated Previews**

  The following previews are now an official part of the API:

  - The GitHub Apps API and endpoints that returned the `performed_via_github_app` property no longer require the `machine-man` preview header.
  - To add and view a lock reason to an issue, you no longer need to use the `sailor-v` preview header.

- **GraphQL Schema Changes**

  - The GraphQL schema changes include backwards-compatible changes, schema previews, and upcoming breaking changes.

VMWARE NETWORK DRIVER CHANGES

- The GitHub Enterprise Server default network adapter type for VMware customers has been changed from E1000 to VMXNET3, starting with release 2.22.0. When upgrading from an earlier release to 2.22.0 or newer, if an E1000 network adapter is detected during the pre-upgrade check, the following message will be displayed at the command line:

  ```
  WARNING: Your virtual appliance is currently using an emulated Intel E1000 network adapter.
  For optimal performance, please update the virtual machine configuration on your VMware host to use the VMXNE
  Proceed with installation? [y/N]
  ```

  The administrator can choose to update the network adapter type to VMXNET3 either before or after the GitHub Enterprise Server upgrade. The virtual appliance will need to be shutdown for this change. Customers should follow the VMware recommended steps for changing the virtual machine network adapter configuration to VMXNET3. Please note that `VMXNET3` will not be an option if the OS version for the virtual appliance is set to `Other Linux (64-bit)`. In that case, the OS version would first need to be changed from `Other Linux (64-bit)` to `Other 2.6.x Linux (64-bit)` or if available, `Debian GNU/Linux 9` . We recommend testing these changes on a staging instance before it is performed on a production GitHub Enterprise Server.

BUG FIXES

- The stafftools page for viewing pending collaborator showed a `500 Internal Server Error` when there was a pending email invite.
- The Repository Health Check in stafftools could give incorrect results on busy repositories.
- A logged in user trying to accept an email invitation could get a `404 Not Found` error.
- If a user navigated to a repository whose name started with "repositories.", they were redirected to the owner's "Repositories" tab instead of landing on the repository overview page.
- Labels in the dashboard timeline did not have enough contrast.

DEPRECATIONS

UPCOMING DEPRECATION OF GITHUB ENTERPRISE SERVER 2.19

- **GitHub Enterprise Server 2.19 will be deprecated as of November 12, 2020** That means that no patch releases will be made, even for critical security issues, after this date. For better performance, improved security, and new features, upgrade to the newest version of GitHub Enterprise Server as soon as possible.

DEPRECATION OF LEGACY GITHUB APP WEBHOOK EVENTS

- Starting with GitHub Enterprise Server 2.21.0 two legacy GitHub Apps-related webhook events have been deprecated and will be removed in GitHub Enterprise Server 2.25.0. The deprecated events `integration_installation` and `integration_installation_repositories` have equivalent events which will be supported. More information is available in the deprecation announcement blog post.

DEPRECATION OF LEGACY GITHUB APPS ENDPOINT

- Starting with GitHub Enterprise Server 2.21.0 the legacy GitHub Apps endpoint for creating installation access tokens was deprecated and will be removed in GitHub Enterprise Server 2.25.0. More information is available in the deprecation announcement blog post.

DEPRECATION OF OAUTH APPLICATION API

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

BACKUPS

- GitHub Enterprise Server 2.22 requires at least GitHub Enterprise Backup Utilities 2.22.0 for Backups and Disaster Recovery.

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.
- The Name ID Format dropdown in the Management Console resets to "unspecified" after setting instance to "persistent".
- The repository Settings page of a repository for a user or organization GitHub Pages sites will fail with a "500 Internal Server Error".
- Users may experience slower Git clone and fetch performance on an instance with high availability replicas due to reads being forwarded to a different node.
- Creating a GitHub App from a manifest fails. To work around this issue, users can follow the manual instructions for creating a GitHub App.
- GitHub usernames may change unintentionally when using SAML authentication, if the GitHub username does not match the value of the attribute mapped to the `username` field in the Management Console. (updated 2020-10-08)
- On a freshly set up 2.22.0 instance or after upgrading to 2.22.0, the activity feed on an organization's dashboard will no longer update. (updated 2020-10-27)
- 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.

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