< 2.22

3.0 Release notes

# Enterprise Server 3.0.3 Download Print

March 23, 2021

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

## SECURITY FIXES

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

## BUG FIXES

- Running `ghe-cluster-config-init` could cause a cluster to become inoperable.
- Resolving merge conflicts in the GUI would fail when custom pre-receive hooks are configured on the repository.
- `launch-deployer` and `launch-receiver` were logging at DEBUG level and filling logs with unnecessary information.
- Systemd could lose track of HAProxy's PID.
- When Actions was configured to use S3 storage, the logs for an action would sometimes fail to load.
- The mysql-failover warning was displayed indefinitely after a successful failover.

- The `ghe-cluster-config-init` run was not fully accounting for the exit code of background jobs leading to improper handling of preflight checks.
- When enabling GitHub Actions, initialization could fail silently.
- When vulnerability alerting is enabled, upgrades to the 3.0 series would fail.
- Jobs related to Codespaces were being enqueued leading to an accumulation of unprocessed jobs.

---

### CHANGES

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

---

### KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support or GitHub Premium Support.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non UTF-8 encoded characters.

- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.

## Enterprise Server 3.0.2 Download Print

March 16, 2021

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

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

### SECURITY FIXES

- Packages have been updated to the latest security versions.

### BUG FIXES

- During a backup an error "Warning: One or more storage objects were not found on the source appliance." was occurring when attempting to clean up purgeable storage objects.
- Dependency graph failed to parse `yarn.lock` JavaScript manifest files, resulting in HTTP 500 errors in logs.
- Disabling GitHub Actions would sometimes fail.
- Custom pre-receive hooks weren't allowed to write to `/tmp` , preventing some scripts from running correctly.
- Systemd journal logs were duplicated in multiple places.
- A timezone set on GitHub Enterprise 11.10.x or earlier was reset to UTC time after upgrading to 3.0 which caused timestamps to shift in some instances.

- Clicking "Publish your first package" in the packages sidebar on a repository would lead to an empty page.
- A site admin could get a 500 error page while trying to view issues referenced from private repositories.
- After disabling GitHub Packages, some organization pages would return an HTTP 500 error response.
- Importing of repository archives from GitHub Enterprise Server that are missing repository files would fail with an error.
- Repository deploy keys were unable to be used with repositories containing LFS objects.
- In the packages sidebar of a repository, the Docker icon was gray and a tool tip displayed "This service is deprecated".
- Webhooks configured with a content type of `application/x-www-form-urlencoded` did not receive query parameters in the POST request body.
- Users could dismiss a mandatory message without checking all checkboxes.
- In some cases after upgrading from a 2.22.X instance, the web interface assets were missing and the page would not render correctly.
- Running `ghe-config-apply` could time out with `Failure waiting for nomad jobs to apply` due to `'job' stanza not found`.

---

KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support or GitHub Premium Support.

- Jupyter Notebook rendering in the web UI may fail if the notebook includes non UTF-8 encoded characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- 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 MainP
     ```

  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
     ```

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

---

---

## Enterprise Server 3.0.1 Download Print

March 02, 2021

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

---

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

### SECURITY FIXES

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

### BUG FIXES

- The load-balancer health checks in some cases could cause the babeld logs to fill up with errors about the PROXY protocol.

- The HTTP headers were not compliant with HTTP RFC standards in specific responses like 304 status for archives.
- On instances that host Python repositories with the Dependency Graph feature enabled, the instance could become unresponsive due to the root disk filling with error logs.
- An informational message was unintentionally logged as an error during GitHub Enterprise Backup Utilities snapshots, which resulted in unnecessary emails being sent when backups were scheduled by cron jobs that listen for output to stderr.
- On VMWare ESX 6.7 the initial configuration could hang while creating host keys which left the instance inaccessible via SSH.
- When GitHub Actions was enabled, disabling maintenance mode in the management console failed.
- The Package creation setting was shown on the organization member settings page, though this feature is not yet available.
- While enabling secret scanning on the Security & Analysis page the dialog incorrectly mentions private repositories.
- When editing a wiki page a user could experience a 500 error when clicking the Save button.
- An S/MIME signed commit using a certificate with multiple names in the subject alternative name would incorrectly show as "Unverified" in the commit badge.
- User saw 500 error when executing git operations on an instance configured with LDAP authentication.
- Suspended user was sent emails when added to a team.
- When a repository had a large number of manifests an error `You have reached the maximum number of allowed manifest files (20) for this repository.` was shown on the Insights -> Dependency graph tab. For more information, see Visualization limits.
- Fixes users being shown the option to set up the Code Scanning CodeQL Action even if Actions was not enabled for their repository.
- The "Prevent repository admins from changing anonymous Git read access" checkbox available in the enterprise account settings could not be successfully enabled or disabled.
- The modal used to display a mandatory message contained no vertical scrollbar, meaning longer messages could not be viewed in full.
- Redis would sometimes fail to start after a hard reboot or application crash.
- Dependency graph fails to parse `setup.py` Python manifest files, resulting in HTTP 500 errors in logs. This, combined with the duplicated logging issue, results in increased root volume utilization.

### CHANGES

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

---

### KNOWN ISSUES

- On a freshly set up GitHub Enterprise Server without any users, an attacker could create the first admin user.
- Custom firewall rules are not maintained during an upgrade.
- Git LFS tracked files uploaded through the web interface are incorrectly added directly to the repository.
- Issues cannot be closed if they contain a permalink to a blob in the same repository where the file path is longer than 255 characters.
- When "Users can search GitHub.com" is enabled with GitHub Connect, issues in private and internal repositories are not included in GitHub.com search results.
- When maintenance mode is enabled, some services continue to be listed as "active processes". The services identified are expected to run during maintenance mode. If you experience this issue and are unsure, contact GitHub Enterprise Support or GitHub Premium Support.
- Duplicated logging to `/var/log/messages` , `/var/log/syslog` , and `/var/log/user.log` results in increased root volume utilization.
- Users can dismiss a mandatory message without checking all checkboxes.
- Pre-receive hook scripts cannot write temporary files, which may cause script execution to fail. Users who use pre-receive hooks should test in a staging environment to see if scripts require write access.
- Repository deploy keys are unable to be used with repositories containing LFS objects.
- Jupyter Notebook rendering in the web UI may fail if the notebook includes non UTF-8 encoded characters.
- reStructuredText (RST) rendering in the web UI may fail and instead display raw RST markup text.
- Dependency graph fails to parse `yarn.lock` Javascript manifest files, resulting in HTTP 500 errors in logs.

- Instances with a custom timezone that were upgraded from an earlier release of GitHub Enterprise Server may have incorrect timestamps in the web UI.
- 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 MainP
     ```

  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
     ```

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

## Enterprise Server 3.0.0 Download Print

February 16, 2021

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

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

SECURITY FIXES

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

---

FEATURES

### GITHUB ACTIONS

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

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

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

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

### GITHUB PACKAGES

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

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

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

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

### GITHUB MOBILE BETA

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

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

### ADVANCED SECURITY SECRET SCANNING BETA

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

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

### ADVANCED SECURITY CODE SCANNING

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

CHANGES

### ADMINISTRATION CHANGES

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

### SECURITY CHANGES

- Organization owners can now disable publication of GitHub Pages sites from repositories in the organization. Disabling GitHub Pages for the organization will prevent members from creating new Pages sites but will not unpublish existing sites. For more information, see "Disabling publication of GitHub Pages sites for your organization."
- A datacenter must be explicitly defined on all nodes before enabling an active replica.
- All usage of SSH fingerprints has been switched to use SHA256 fingerprints as they are used with OpenSSH since version 6.8 as well. This applies to the web interface and also the API where

fingerprints are returned such as in GraphQL. The fingerprints follow the OpenSSH format.

- SHA-1 and SHA-256 signature headers (two headers) are sent on webhooks.

### DEVELOPER CHANGES

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

### API CHANGES

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

### DEFAULT BRANCH RENAMING

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

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

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

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

## BUG FIXES

### FIXES FOR KNOWN ISSUES FROM RELEASE CANDIDATES

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

### FIXES FOR OTHER ISSUES

- Issues with migrations and upgrades to 3.0.0 have been fixed.
- Backup Utilities versioning now works for release candidate versions.
- Generating a support bundle resulted in an error in the orchestrator logs.
- A large restore could result in Redis running out of memory.
- The checkbox to enable GitHub Actions in the Management Console is now visible with any authentication method.
- GitHub Actions could be enabled if the required storage was also configured.
- `ghe-repl-status` could silently fail if MSSQL replication was not configured.
- The format of several log files have changed, including the addition of a PID for different log types. This does not affect how GitHub Enterprise Support uses support bundles to troubleshoot issues.
- A PATCH request to the webhook configuration API no longer erases the webhook secret.
- Certain types of pre-receive hooks were failing.
- The Packages NuGet service now normalizes semantic versions on publish. An invalid semantic version (for example: v1.0.0.0.0.0) is not downloadable by NuGet clients and therefore a NuGet service is expected to normalize those versions (for example: v1.0.0.0.0.0 --> v1.0.0). Any original, non-normalized, version will be available in the `verbatimVersion` field. No changes to client configurations are required.

## KNOWN ISSUES

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

---

DEPRECATIONS

### DEPRECATION OF GITHUB ENTERPRISE SERVER 2.19

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

### DEPRECATION OF LEGACY GITHUB APP WEBHOOK EVENTS

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

### DEPRECATION OF LEGACY GITHUB APPS ENDPOINT

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

### DEPRECATION OF OAUTH APPLICATION API

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

### DEPRECATION OF SUPPORT FOR SEMIOTIC

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

### DEPRECATION OF WORKFLOW COMMANDS

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

BACKUPS

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