Enterprise Server 3.10.3

Download GitHub Enterprise Server 3.10.3

October 24, 2023

Warning: A change to MySQL in GitHub Enterprise Server 3.9 and later may impact the performance of your instance. Before you upgrade, make sure you've read the "Known issues" section of these release notes.

3.10.3: Security fixes

- **HIGH:** Due to an incorrect permission assignment for some configuration files, an attacker with access to a local operating system user account could read MySQL connection details including the MySQL password. GitHub has requested CVE ID CVE-2023-23767 for this vulnerability.
- Packages have been updated to the latest security versions.

3.10.3: Bug fixes

- Authentication of programmatic access token's did not fully validate the status of token's users, which allowed token authentication requests to succeed even if the associated user was not allowed to make such requests. This issue is unrelated to validation of token scope.
- The `dependency-graph-api` service sometimes rapidly filled logs with a large amount of Base64-encoded response data, particularly during upgrades.
- After an administrator made changes to maintenance mode from the instance's Management Console UI using Firefox, the administrator was redirected to the Settings page, but their changes were not enabled.
- The `ghe-cluster-repl-status` command did not display all replication statuses.
- On an instance in a cluster configuration with high availability enabled, `ghe-config-apply` timed out while waiting for `hookshot-go` to start on replica application nodes.
- `/var/log/lastlog` was not copied over as a sparse file during `ghe-upgrade`, which could cause issues by using additional disk space.
- On an instance in a cluster configuration, when managing maintenance mode using `ghe-cluster-maintenance`, an erroneous warning appeared that read "Warning: Maintenance mode set on primary, please make sure to set it on any active replica if needed".
- `ghe-repl-status` did not identify Git replicas in certain incomplete states and incorrectly suggested that a failover could be performed safely. In some cases, this led to data loss during failover.
- Repository exports using `ghe-migrator` or the REST API's operation for organization migrations could fail when a large number of commit comments or long commit comments were present.

- On an instance with a GitHub Advanced Security license and secret scanning enabled, secret scanning suggested incorrect filters when viewing both open and closed alerts.
- On instances using the private beta of SCIM provisioning, some users were presented with a "single sign-in" hover card.
- On an instance with multiple nodes, `ghe-spokes status` did not identify Git replicas in certain incomplete states, causing a false report that replication was in sync and leading to data loss or replication issues during failover.
- On an instance with GitHub Actions enabled, administrators received a `500` error after attempting to force cancel a workflow run via Staff Tools.
- On an instance with a GitHub Advanced Security license, repositories within organizations created using the `+` dropdown menu did not have GitHub Advanced Security features enabled automatically, even if the features should have been enabled.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, dry runs sometimes incorrectly reported no results for custom patterns.

3.10.3: Changes

- Instructions in the "Migrations" section of the Management Console clarify that only standard AWS S3 endpoints are supported when configuring AWS S3 as a blob storage provider for migrations.
- On an instance in a cluster configuration, administrators can identify the repository networks or gists that are common across a specified set of storage nodes using the `spokesctl find-on-replicas` command.
- As a security measure, GitHub Pages does not build sites that contain symbolic links except when using custom GitHub Actions workflows. This change strengthens GitHub Pages's symbolic link detection.

3.10.3: Known issues

- Custom firewall rules are removed during the upgrade process.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see "Troubleshooting access to the Management Console."
- On an instance in a high-availability configuration, passive replica nodes accept Git client requests and forward the requests to the primary node.
- If an instance is configured to forward logs to a target server with TLS enabled, certificate authority (CA) bundles that a site administrator uploads using `ghe-ssl-ca-certificate-install` are not respected, and connections to the server fail.
- When running `ghe-config-apply`, the process may stall with the message `Deployment`

`is running pending automatic promotion`.

- The `mbind: Operation not permitted` error in the `/var/log/mysql/mysql.err` file can be ignored. MySQL 8 does not gracefully handle when the `CAP_SYS_NICE` capability isn't required, and outputs an error instead of a warning.
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8, to 3.9 or 3.10, MySQL may not start back up. For more information, see "Known issues with upgrades to your instance." [Updated: 2023-08-11]
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8 to 3.9 or 3.10, I/O utilization will increase, and in some cases the instance's performance will be impacted. Reduced performance is due to the database server being upgraded from MySQL 5.7 to MySQL 8.0. For more information, see "Known issues with upgrades to your instance."
- In rare circumstances, a small instance with both high availability and GitHub Actions configured may report that MSSQL replication is unhealthy after many upgrades with full upgrade packages. If you encounter this issue, contact GitHub Support.
- On an instance in a cluster configuration with high availability configured, `ghe-config-apply` times out while waiting for `hookshot-go` to start on replica application nodes.
- After an administrator enables maintenance mode from the instance's Management Console UI using Firefox, the administrator is redirected to the Settings page, but maintenance mode is not enabled. To work around this issue, use a different browser.
- When an administrator uses the `-p` flag with the `ghe-support-bundle` utility to collect data for a specific number of hours, the utility erroneously collects more logs than necessary.
- When an administrator uses the `-p` flag with the `ghe-support-bundle` utility to collect data for a specific number of hours, the utility erroneously collects more logs than necessary.

Enterprise Server 3.10.2

Download GitHub Enterprise Server 3.10.2

September 22, 2023

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

Warning: A change to MySQL in GitHub Enterprise Server 3.9 and later may impact the performance of your instance. Before you upgrade, make sure you've read the "Known issues" section of these release notes.

3.10.2: Bug fixes

- On an instance in a high-availability, geo-replication, or repository cache configuration, prolonged replication issues could occur on replica nodes due to failure of `SpokesRepairRepoReplicaJob` and `SpokesSyncCacheReplicaJob` jobs.

3.10.2: Known issues

- Custom firewall rules are removed during the upgrade process.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see "Troubleshooting access to the Management Console." [Updated: 2023-02-23]
- On an instance in a high-availability configuration, passive replica nodes accept Git client requests and forward the requests to the primary node.
- If an instance is configured to forward logs to a target server with TLS enabled, certificate authority (CA) bundles that a site administrator uploads using `ghe-ssl-ca-certificate-install` are not respected, and connections to the server fail.
- When running `ghe-config-apply`, the process may stall with the message `Deployment is running pending automatic promotion`.
- The `mbind: Operation not permitted` error in the `/var/log/mysql/mysql.err` file can be ignored. MySQL 8 does not gracefully handle when the `CAP_SYS_NICE` capability isn't required, and outputs an error instead of a warning.
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8, to 3.9 or 3.10, MySQL may not start back up. For more information, see "Known issues with upgrades to your instance." [Updated: 2023-08-11]
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8 to 3.9 or 3.10, I/O utilization will increase, and in some cases the instance's performance will be impacted. Reduced performance is due to the database server being upgraded from MySQL 5.7 to MySQL 8.0. For more information, see "Known issues with upgrades to your instance."
- In rare circumstances, a small instance with both high availability and GitHub Actions configured may report that MSSQL replication is unhealthy after many upgrades with full upgrade packages. If you encounter this issue, contact GitHub Support.
- On an instance in a cluster configuration with high availability configured, `ghe-config-apply` times out while waiting for `hookshot-go` to start on replica application nodes.
- After an administrator enables maintenance mode from the instance's Management Console UI using Firefox, the administrator is redirected to the Settings page, but maintenance mode is not enabled. To work around this issue, use a different browser.
- When an administrator uses the `-p` flag with the `ghe-support-bundle` utility to collect data for a specific number of hours, the utility erroneously collects more logs than necessary. [Updated: 2023-10-13]
- The settings for enabling scheduled reminders were added unintentionally to this release. Scheduled reminders are not officially supported. [Updated: 2023-10-17]

Enterprise Server 3.10.1

Download GitHub Enterprise Server 3.10.1

September 21, 2023

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

Warnings:

- This release contains a known issue that may lead to replication issues on an instance in a high-availability, geo-replication, or repository cache configuration. Upgrade to GitHub Enterprise Server 3.10.2 or later instead of this release. For more information, see the "Known issues" section of these release notes.
- A change to MySQL in GitHub Enterprise Server 3.9 and later may impact the performance of your instance. Before you upgrade, make sure you've read the "Known issues" section of these release notes.

3.10.1: Security fixes

- HTTP Strict Transport Security (HSTS) is enabled within the Management Console.
- Packages have been updated to the latest security versions.
- **LOW:** An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff in a reopened pull request. To exploit this vulnerability, an attacker would need write access to the repository. This vulnerability was reported via the GitHub Bug Bounty program and was assigned CVE-2023-23766. [Updated: 2023-09-22]

3.10.1: Bug fixes

- On an instance with GitHub Actions enabled, scale sets configured at the enterprise level did not appear for use within the instance's organizations or repositories.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, secret scanning alerts could fail to show an error message in the UI when a failure occurred closing or reopening the alert.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, and when using Safari, changing additional match requirements for a custom pattern did not retrigger custom pattern evaluation against a user submitted test string.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, organization access for a leaked GitHub tokens was not shown to commit authors when viewing the alert.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, when token location(s) included a commit that introduced a large change, the page for viewing the alert would load slowly.
- When uploading migration archives to blob storage, the GitHub Enterprise Server instance's outbound web proxy server was not used.
- On an enterprise with the policy setting that disallows repository admins from enabling/disabling secret scanning, transferring a repository to a new organization that automatically enabled secret scanning wouldn't result in the transferred repository being automatically enabled for secret scanning.
- When migrating a repository from a GitHub Enterprise Server instance to another location, the `ghe-migrator target_url` command allows you to record the repository's

new location. The new URL is displayed when you visit the main page of the repository in the web interface.

- On an instance with subdomain isolation disabled, a notebook could not be loaded due to incorrect asset paths.
- On an instance with a GitHub Advanced Security license and secret scanning enabled, in some cases, custom patterns would erroneously show no results for a dry run.

3.10.1: Changes

- When GitHub Enterprise checks for a new upgrade or hotpatch package, if the check fails the failure details are output to the `ghe-update-check` log, and the Management Console UI provides a "Check Again" button to rerun the check.
- When providing data to GitHub Support, GitHub Enterprise Server displays a notice describing how support data is used before uploading the support files.

3.10.1: Known issues

- Custom firewall rules are removed during the upgrade process.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account does not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see "Troubleshooting access to the Management Console." [Updated: 2023-02-23]
- On an instance in a high-availability configuration, passive replica nodes accept Git client requests and forward the requests to the primary node.
- If an instance is configured to forward logs to a target server with TLS enabled, certificate authority (CA) bundles that a site administrator uploads using `ghe-ssl-ca-certificate-install` are not respected, and connections to the server fail.
- When running `ghe-config-apply`, the process may stall with the message `Deployment is running pending automatic promotion`.
- The `mbind: Operation not permitted` error in the `/var/log/mysql/mysql.err` file can be ignored. MySQL 8 does not gracefully handle when the `CAP_SYS_NICE` capability isn't required, and outputs an error instead of a warning.
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8, to 3.9 or 3.10, MySQL may not start back up. For more information, see "Known issues with upgrades to your instance." [Updated: 2023-08-11]
- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8 to 3.9 or 3.10, I/O utilization will increase, and in some cases the instance's performance will be impacted. Reduced performance is due to the database server being upgraded from MySQL 5.7 to MySQL 8.0. For more information, see "Known issues with upgrades to your instance."
- In rare circumstances, a small instance with both high availability and GitHub Actions

configured may report that MSSQL replication is unhealthy after many upgrades with full upgrade packages. If you encounter this issue, contact GitHub Support.

- On an instance in a cluster configuration with high availability configured, `ghe-config-apply` times out while waiting for `hookshot-go` to start on replica application nodes.
- After an administrator enables maintenance mode from the instance's Management Console UI using Firefox, the administrator is redirected to the Settings page, but maintenance mode is not enabled. To work around this issue, use a different browser.
- On an instance with a high-availability, geo-replication, or repository cache configuration, a known issue causes the `SpokesRepairRepoReplicaJob` and `SpokesSyncCacheReplicaJob` jobs to fail. This means repository replicas in cache servers are not updated, and will remain out of sync if the repository is updated. Additionally, if a regular repository replica becomes out of sync, repair attempts will fail, causing the corresponding repository network to be marked as failed until a network repair is triggered.

  The network repair will eventually return the repository to a healthy state. However, this process can take several hours for very large and active repositories or networks, potentially leading to prolonged replication issues. [Updated: 2023-09-26]
- When an administrator uses the `-p` flag with the `ghe-support-bundle` utility to collect data for a specific number of hours, the utility erroneously collects more logs than necessary. [Updated: 2023-10-13]
- The settings for enabling scheduled reminders were added unintentionally to this release. Scheduled reminders are not officially supported. [Updated: 2023-10-17]

Enterprise Server 3.10.0

Download GitHub Enterprise Server 3.10.0

August 29, 2023

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

For upgrade instructions, see "Upgrading GitHub Enterprise Server."

Warnings:

- This release contains a known issue that may lead to replication issues on an instance in a high-availability, geo-replication, or repository cache configuration. The issue is resolved in GitHub Enterprise Server 3.10.2 and later. For more information, see the "Known issues" section of these release notes.
- A change to MySQL in GitHub Enterprise Server 3.9 and later may impact the performance of your instance. Before you upgrade, make sure you've read the "Known issues" section of these release notes.

3.10.0: Features

- **Instance administration**
  - To monitor the status of migrations in more detail, users with administrative SSH

access to an instance can use the `ghe-migrations` utility to see the progress of individual migration groups. For more information, see "Command-line utilities."

- Site administrators can set a custom message for their users to see during a maintenance window. For more information, see "Enabling and scheduling maintenance mode."
- Site administrators can use the Manage GitHub Enterprise Server API to view and manage the maintenance status of an instance, including setting an IP exception list and modifying the message displayed to users during a maintenance window. For more information, see "Manage GitHub Enterprise Server" in the REST API documentation.
- Site administrators can use the Manage GitHub Enterprise Server API to change the `site admin` password and to make changes to management console users. For more information, see "Manage GitHub Enterprise Server" in the REST API documentation.

- **Authentication**
  - To help users access resources more securely, fine-grained personal access tokens are available in public beta. For more information, see "Managing your personal access tokens."
    - Users can create fine-grained personal access tokens with access to their personal repositories or, if permitted, organization-owned repositories.
    - Organization and enterprise owners can enable or disable the use of fine-grained personal access tokens in organization-owned repositories, and can use the REST API or GraphQL API to manage tokens in their organizations.
    - Users creating fine-grained tokens for an organization can add the `pre-receive hooks` permission to allow managing pre-receive hooks. For more information, see "Managing pre-receive hooks on your instance."

- **GitHub Advanced Security**
  - To find vulnerabilities in specific parts of a project, users with write access to a repository can filter code scanning alerts by language or by file path by using the search queries `language:` and `path:`. For more information, see "Managing code scanning alerts for your repository."
  - To help repository administrators and security managers quickly enable automatic code scanning without needing to configure a workflow, default setup for code scanning supports compiled languages including Go, Java, and C. Default setup is now available for all languages supported by CodeQL, except Swift. For more information, see "CodeQL code scanning for compiled languages" and Supported languages and frameworks in the CodeQL documentation.
  - Repository administrators and security managers can choose which languages to include or exclude in default setup for code scanning. For more information, see "Configuring default setup for code scanning."
  - To improve analysis of C# code, the release of CodeQL included with GitHub Enterprise Server 3.10 can scan projects that include features from C# 11. For more information, see What's new in C# 11 in the Microsoft documentation. Support for C# 11 is in beta and subject to change. CodeQL can scan projects built with C# 11 features, but does not analyse the code used for C# 11 features themselves.
  - To help users find vulnerabilities in projects for Swift libraries and Apple apps, the release of CodeQL included with GitHub Enterprise Server 3.10 includes support for Swift, up to version 5.8.1, and Xcode, up to version 14.3.1. Support for Swift is in

beta and subject to change. Swift analysis is not supported in default setup for code scanning, and requires the advanced setup. For more information, see "Configuring code scanning."

  - To help identify steps to remediate leaked secrets, repository administrators and security managers can view metadata such as the secret owner, expiration date, and access rights for any active GitHub token leaked in a repository. This feature is in beta and subject to change. For more information, see "Managing alerts from secret scanning."

  - Repository administrators, security managers, and organization and enterprise owners can view metrics for alerts generated by a specific custom pattern for secret scanning. This feature is in beta and subject to change. For more information, see "Defining custom patterns for secret scanning."

- **Dependabot**

  - Dependabot can automatically update the version of Node.js dependencies managed in the pnpm package manager. For more information, see "About Dependabot version updates."

  - To avoid unnecessary compute cost, Dependabot updates are automatically paused in repositories where there has been no activity on pull requests created by Dependabot for 90 days. For more information about the criteria for Dependabot updates being paused, see "About Dependabot security updates" and "About Dependabot version updates."

  - To avoid unnecessary compute cost, Dependabot stops automatically rebasing a pull request for version or security updates if the pull request has been open for 30 days.

- **Code security**

  - In the GitHub Advisory Database, users can search for any historical vulnerability recognized by the National Vulnerability Database. The "Unreviewed advisories" category has been backfilled to include vulnerabilities from previous years. For more information, see "Browsing security advisories in the GitHub Advisory Database."

  - In the GitHub Advisory Database, users can search for malware advisories by using the query `type:malware`. Dependabot does not send alerts for malware advisories. For more information, see "Browsing security advisories in the GitHub Advisory Database."

  - In the GitHub Advisory Database, users can search for advisories for the Hex package manager, including Elixir, Erlang, and more. Dependabot does not send alerts for Hex advisories. For more information, see "Browsing security advisories in the GitHub Advisory Database."

  - Organization owners, security managers, and users with admin access to a repository can quickly enable or disable security features for a filtered selection of repositories from the "Security coverage" view in an organization's security overview. This feature is in beta and subject to change. For more information, see "Enabling security features for multiple repositories."

  - Enterprise owners, organization owners, and security managers can quickly assess adoption of security features and exposure to security vulnerabilities across their enterprise. The enterprise-level "Security coverage" and "Security risk" views in security overview display data for repositories in each organization where the viewer is an organization owner or security manager. These views replace the "Overview" page in the "Code Security" tab for an enterprise. The `risk` metric for

filtering the "Overview" page is no longer available. This feature is in beta and subject to change. For more information, see "About security overview."

- Users can find curated security advisories for the Swift ecosystem in the GitHub Advisory Database. For more information, see "About the GitHub Advisory database."

- **GitHub Actions**
  - Organization owners can increase instance security by preventing members from creating self-hosted runners at the repository level. For more information, see "Disabling or limiting GitHub Actions for your organization."
  - Users with admin access to a repository can allow external systems and third-party services to approve or reject deployments across organizations, repositories, and environments by enabling custom deployment protection rules. This feature is in beta and subject to change. For more information, see "Using environments for deployment."
  - The option to execute custom scripts on a self-hosted runner is no longer is beta. For more information, see "Running scripts before or after a job."
  - To prevent unnecessary transfer of OIDC tokens between workflows, to fetch an OIDC token generated within a reusable workflow that is outside their enterprise or organization, users must set the `id-token` permission to `write` in the workflow or specific job where the reusable workflow is called. For more information, see "Configuring OpenID Connect in cloud providers."
  - Repository administrators, organization owners, and users with the `manage_runners:enterprise` scope for enterprises can use the REST API to create ephemeral, just-in-time (JIT) runners that can perform at most one job before being automatically removed from the repository, organization, or enterprise. For more information, see "Security hardening for GitHub Actions."

- **Community experience**
  - To improve the accuracy of marked answers in discussions, and reduce the burden on users to duplicate their text to get their answer marked as correct, users can mark threaded replies as the answer to a question.
  - To improve content organization and topic discoverability, GitHub Discussions maintainers can group discussion categories into sections.

- **Repositories**
  - To prevent unnecessary repository removal, the API for managing the repositories accessible by a GitHub App in your organization has been updated to fail early if the application is currently granted access to `all` repositories in the organization. This API can only be used to remove a repository when the application has been granted access to an explicit list of repositories. For more information, see "GitHub App installations."
  - Repository administrators can ensure the security and stability of branches by requiring pull request approval by someone other than the last pusher. For more information, see "About protected branches."

- **Projects**
  - Projects is no longer in public beta, and is now considered generally available. For more information, see "About Projects."

- To control the amount of work in progress and promote focus, on a board layout, users with admin access to a project can set a recommended limit on the number of items in a column. For more information, see "Customizing the board layout."
- To determine the default access rights organization members have to projects where they haven't been granted individual access, organization owners can set a base role for projects. For more information, see "Managing access to your projects."
- To share a pre-configured project with other people in an organization, users with admin access to a project can set the project as a template. This feature is in beta and subject to change. For more information, see "Managing project templates in your organization."
- In a table layout, users can select and update multiple cells at once by clicking and dragging or using the `Shift` or `Ctrl` / `Command` key.

- **Commits**
  - When editing a file in the user interface, users with permission to bypass branch protection rules receive a note if their commit will bypass a rule, with the option to create a new branch instead of committing directly to the protected branch. Previously, the commit was added to the protected branch directly, without indication that a rule was being bypassed.
  - When using `git push` from the command line, users with permission to bypass branch protection rules receive a note if they have pushed a commit that bypasses a rule. Previously there was no indication after a Git push that branch rules had been bypassed.

- **Markdown**
  - Users can include mathematical expressions within Markdown by using LaTeX syntax delimited by `$` characters and backticks. For more information, see "Writing mathematical expressions."

- **Accessibility**
  - To make GitHub inclusive to all developers, GitHub has improved color contrast of the default light and dark themes, making them accessible to all users. These changes were made to Primer, GitHub's Design System. For more information, see GitHub Accessibility.

3.10.0: Changes

- Field names and destinations for some service logs on GitHub Enterprise Server have changed in this release and the prior release. If any tooling or processes in your environment rely on specific field names within logs, or log entries in specific files, the following changes may affect you.
  - `level` is now `SeverityText`.
  - `log_message`, `msg`, or `message` is now `Body`.
  - `now` is now `Timestamp`.
  - Custom field names such as `gh.repo.id` or `graphql.operation.name` use semantic names.
  - Log statements that the instance would previously write to `auth.log`, `ldap.log`, or `ldap-sync.log` now appear in containerized logs for `github-unicorn` if the statement originated from a web request, or in logs for `github-resqued` if the statement originated from a background job. For more information about

containerized logs, see "About system logs."

For a full list of field mappings, download the OpenTelemetry attribute mapping CSV for GitHub Enterprise Server 3.9 and the OpenTelemetry attribute mapping CSV for GitHub Enterprise Server 3.10. This change is part of GitHub's gradual migration to internal semantic conventions for OpenTelemetry, and additional field names will change in upcoming releases.

- Users who use pull requests with protected branches may be affected by the following security measures.
  - Merge commits created locally and pushed to a protected branch are rejected if the contents of the commit differ from the merge commit predicted by GitHub.
  - If the branch protection rule for dismissing stale reviews is active, an approving review is dismissed if the merge base changes after the review was submitted. The merge base is the commit that is the latest common ancestor of the pull request branch and the protected branch.
  - A pull request approval only counts towards the pull request it was submitted for. Previously, approvals were gathered across multiple independent pull requests if the pull request branches pointed to the same commit and targeted the same base branch.
- The `PUT` and `DELETE` operations on the `/installations/{installation_id}/repositories/{repository_id}` endpoint are no longer functional for the management of GitHub App installations. You can add or remove a repository from an app installation using the documented APIs instead. For more information, see "GitHub App installations."
- On an instance with a GitHub Advanced Security license, to make it easier to assess vulnerabilities to exposed secrets, enterprise owners and organization owners receive a single email with the results of the historical scan for secrets that is performed when secret scanning is first enabled in an organization or enterprise. Previously, secret scanning sent an email for each repository where secrets were detected. For more information, see "About secret scanning."
- On an instance with a GitHub Advanced Security license, in the "Files changed" view of pull requests, GitHub only displays code scanning alerts for vulnerabilities detected in lines that a pull request has changed. Previously, code scanning displayed all alerts unique to the pull request branch, even if they were unrelated to the changes the pull request introduced.

3.10.0: Backups

- To generate backups of an instance more quickly, in GitHub Enterprise Server Backup Utilities 3.10.0 and later, the job for pruning snapshots is no longer performed as part of the `ghe-backup` tool. Site administrators can prune snapshots manually or on a schedule by running the `ghe-prune-snapshots` job. For more information, see Scheduling backups in the `github/backup-utils` repository.
- To reduce the data transfer required to regularly back up an instance, GitHub Enterprise Server Backup Utilities 3.10.0 and later allows administrators to perform incremental backups of a MySQL 8 database. For more information, see Making a Differential or Incremental Backup in the MySQL documentation.

3.10.0: Known issues

- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8 to 3.9 or 3.10, I/O utilization will increase, and in some cases the instance's performance will be impacted. Reduced performance is due to the database server being upgraded from MySQL 5.7 to MySQL 8.0. For more information, see "Known issues with upgrades to

your instance."

- After an administrator upgrades from GitHub Enterprise Server 3.7 or 3.8, to 3.9 or 3.10, MySQL may not start back up. For more information, see "Known issues with upgrades to your instance." [Updated: 2023-08-11]
- When enabling CodeQL via default setup at scale, some checks related to GitHub Actions are omitted, potentially preventing the process from completing.
- On an instance in a cluster configuration, after you upgrade nodes other than the primary MySQL node and before you upgrade the primary MySQL node, the following output may appear multiple times after you run `ghe-config-apply`.

  ```
  Error response from daemon: conflict: unable to delete IMAGE_ID (cannot be
  forced) - image is being used by running container CONTAINER_ID
  ```

  You can safely ignore this message.
- Custom firewall rules are removed during the upgrade process.
- The GitHub Packages npm registry no longer returns a time value in metadata responses. This was done to allow for substantial performance improvements. We continue to have all the data necessary to return a time value as part of the metadata response and will resume returning this value in the future once we have solved the existing performance issues.
- On an instance in a high-availability configuration, passive replica nodes accept Git client requests and forward the requests to the primary node.
- The `mbind: Operation not permitted` error in the `/var/log/mysql/mysql.err` file can be ignored. MySQL 8 does not gracefully handle when the `CAP_SYS_NICE` capability isn't required, and outputs an error instead of a warning.
- When using an outbound web proxy server, the `ghe-btop` command may fail in some circumstances with the error "Error querying allocation: Unexpected response code: 401".
- If an instance is configured to forward logs to a target server with TLS enabled, certificate authority (CA) bundles that a site administrator uploads using `ghe-ssl-ca-certificate-install` are not respected, and connections to the server fail.
- When running `ghe-config-apply`, the process may stall with the message `Deployment is running pending automatic promotion`.
- During the validation phase of a configuration run, a `No such object` error may occur for the Notebook and Viewscreen services. This error can be ignored as the services should still correctly start.
- If the root site administrator is locked out of the Management Console after failed login attempts, the account will not unlock automatically after the defined lockout time. Someone with administrative SSH access to the instance must unlock the account using the administrative shell. For more information, see "Troubleshooting access to the Management Console."
- In rare circumstances, a small instance with both high availability and GitHub Actions configured may report that MSSQL replication is unhealthy after many upgrades with full upgrade packages. If you encounter this issue, contact GitHub Support. [Updated: 2023-09-04]
- After an administrator enables maintenance mode from the instance's Management Console UI using Firefox, the administrator is redirected to the Settings page, but maintenance mode is not enabled. To work around this issue, use a different browser. [Updated: 2023-09-19]

- On an instance in a cluster configuration with high availability configured, `ghe-config-apply` times out while waiting for `hookshot-go` to start on replica application nodes. [Updated: 2023-09-21]
- On an instance with a high-availability, geo-replication, or repository cache configuration, a known issue causes the `SpokesRepairRepoReplicaJob` and `SpokesSyncCacheReplicaJob` jobs to fail. This means repository replicas in cache servers are not updated, and will remain out of sync if the repository is updated. Additionally, if a regular repository replica becomes out of sync, repair attempts will fail, causing the corresponding repository network to be marked as failed until a network repair is triggered.

  The network repair will eventually return the repository to a healthy state. However, this process can take several hours for very large and active repositories or networks, potentially leading to prolonged replication issues. [Updated: 2023-09-26]
- When an administrator uses the `-p` flag with the `ghe-support-bundle` utility to collect data for a specific number of hours, the utility erroneously collects more logs than necessary. [Updated: 2023-10-13]
- The settings for enabling scheduled reminders were added unintentionally to this release. Scheduled reminders are not officially supported. [Updated: 2023-10-17]

3.10.0: Deprecations

- **Upcoming deprecation of team discussions**
  - GitHub will deprecate team discussions for users in GitHub Enterprise Server 3.12. In GitHub Enterprise Server 3.10, a banner appears atop teams' discussions with information about the deprecation, including a link to tooling to migrate existing team discussions to GitHub Discussions. For more information, see "About team discussions" and "About discussions."