Enterprise Server 3.20.1

Download GitHub Enterprise Server 3.20.1

April 21, 2026

3.20.1: Security fixes

- **HIGH**: An attacker could gain unauthorized access to private repositories by abusing scoped user-to-server (`ghu_`) tokens after their associated GitHub App installation was revoked or deleted. In certain cases, the authorization layer could incorrectly fall back to a global installation context instead of rejecting the request, allowing the token to access resources outside its intended installation or repository scope. This issue could be chained with weaknesses in token revocation timing and SSH push attribution to obtain a victim-scoped token and read private repository contents without victim interaction. GitHub has requested CVE ID CVE-2026-5845 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker could extract sensitive environment variables from a GitHub Enterprise Server instance through a timing side-channel attack against the notebook rendering service. When private mode was disabled, the notebook viewer followed HTTP redirects without revalidating the destination host, enabling an unauthenticated Server-Side Request Forgery (SSRF) to internal services. By measuring response time differences, an attacker could infer secret values character by character. GitHub has requested CVE ID CVE-2026-5921 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: A Management Console administrator could inject shell metacharacters into configuration fields via the Management Console configuration API, leading to arbitrary command execution on the appliance as the admin OS user. GitHub has requested CVE ID CVE-2026-4821 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **HIGH**: An attacker with knowledge of a target applications registered OAuth callback URL could gain unauthorized access to user accounts by exploiting incorrect regular expression matching

in callback URL validation. GitHub has requested CVE ID CVE-2026-4296 for this vulnerability, which was reported via the GitHub Bug Bounty program.

- **HIGH**: An attacker without write access could merge their own pull request into a repository that allowed forks by exploiting an incorrect authorization check in the `enable_auto_merge` mutation for pull requests. Exploitation required a clean pull request status and only applied to branches without branch protection rules enabled. GitHub has requested CVE ID CVE-2026-1999 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An attacker with permission to manage secret scanning push protection settings in one repository could add or remove delegated bypass reviewers in a different repository by exploiting an incorrect authorization check in the `/settings/security_analysis/bypass_reviewers` endpoints. Authorization was checked against the repository in the URL route, but the action was applied to a different repository specified in the request body. The impact is limited to assigning existing trusted users as bypass reviewers. GitHub has requested CVE ID CVE-2026-3307 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **MEDIUM**: An authenticated attacker could determine the names of private repositories by their numeric ID through the mobile upload policy API endpoint, which returned repository names in validation error messages without verifying the caller's access. GitHub has requested CVE ID CVE-2026-5512 for this vulnerability, which was reported via the GitHub Bug Bounty program.
- **LOW**: An attacker could create or modify organization rulesets because Security Managers had unintended access. To mitigate this issue, GitHub updated role-based access controls to prevent Security Managers from changing rulesets. This vulnerability was reported via the GitHub Bug Bounty program.

3.20.1: Bug fixes

- Dependabot security updates now work correctly for repositories using grouped security updates on GHES. Previously, an incorrect internal API URL caused security update jobs to fail silently when dependency groups with `applies-to: security-updates` were configured.
- After administrators installed or removed a custom certificate authority (CA) certificate with `ghe-ssl-ca-certificate-install`, Dependabot services continued using the previous CA store and could fail to connect to external registries that required the updated CA.
- On an instance with GitHub Actions enabled, diagnostic log files for storage connectivity checks did not persist to disk when site administrators clicked **Test storage settings** in the management console or ran `ghe-config-apply` to apply configuration changes. This made

storage connection failures difficult to troubleshoot because logs were unavailable in support bundles.

- During initial setup of a new instance, site administrators saw an "Oops! A configuration run is already in progress" error message in the Management Console even though `ghe-config-apply` had not been run.
- On instances using the new OpenTelemetry-based metrics stack, upgrading the instance re-enabled the legacy collectd-based metrics stack.
- Cluster administrators experienced `ghe-config-apply` failures when all replica nodes were marked offline and unreachable. Previously, `ghe-cluster-config-update` attempted to sync configuration files to an empty host list, causing the sync step to fail.
- Administrators experienced `ghe-support-bundle` appearing to hang on instances configured for high availability when one or more replica nodes were offline or unreachable during connectivity checks.
- When Consul replication fails to start, a misleading error message `exit: check_consul_replication: numeric argument required` would be emitted to ghe-config.log.
- On instances with Dependabot enabled, hotpatch upgrades could lock the Nomad jobs queue.
- When site administrators set the `observability.otelcol.gogc-enabled` parameter to a boolean value, the `config-apply` failed.
- API consumers could not access secret scanning scan history for archived repositories, even when the organization had a GitHub Advanced Security license.
- When applying a hotpatch or running a configuration with `ghe-config-apply`, the configuration run could fail with "ERROR: Restoring CodeQL Action release tags" if internal Git services were not yet fully available. The error message "SpokesAPI::TwirpServerError: unavailable" appeared in logs.
- On instances connected to GitHub Enterprise Cloud with data residency, the "GitHub.com actions" setting appeared in the GitHub Connect configuration despite this feature not being available for data residency deployments.
- On instances with GitHub Actions enabled, errors appeared in logs related to missing Elasticsearch field mappings for workflow runs. The workflow run data included an `archived` field that was not defined in the Elasticsearch index mapping.
- The GitHub Enterprise Server staffbar was displaying debugging information used by GitHub.

- On an instance with a GitHub Advanced Security license, searching for assignees in secret scanning alerts did not return results for users with write access if the repository had more than 1500 eligible users.
- Suspended users were listed in an organizations list of members.
- Migrations to GitHub Enterprise Server failed when the importer service tried to import a pull request review comment that referenced a garbage-collected commit. Now, these comments are skipped gracefully.
- After an instance upgraded to a previous patch release in this series, some users dashboard RSS/Atom feeds (`/:login.private.atom`) returned an empty feed with no entries, and users could not subscribe to the feed. Dashboard feeds now return entries as expected.
- The site admin "All organizations" report included soft-deleted organizations.
- Users saw a “Preview” label for secret scanning’s Generic Secrets and Low Confidence Patterns, even though both features were generally available.
- On instances that blocked outbound internet access, code scanning repeatedly failed due to unnecessary outbound requests for functionality that is not available on GitHub Enterprise Server.

3.20.1: Changes

- To improve SSH security, the instance no longer advertises the ssh-rsa signature algorithm (which uses SHA-1) for server host keys on ports 22 and 122. RSA keys continue to work using the more secure rsa-sha2-256 and rsa-sha2-512 signature algorithms. Administrators using very old SSH clients that only support SHA-1 signatures may need to upgrade their clients. For more information about SSH algorithms, see AUTOTITLE.
- Administrators can now set `mysql.innodb-online-alter-log-max-size` with `ghe-config` so the value persists when a configuration is applied or upgraded.
- Administrators can configure the maximum number of concurrent HTTP/2 streams per connection for HAProxy. To set this value, use `ghe-config core.haproxy-h2-max-concurrent-streams VALUE` and run `ghe-config-apply`. Previously, this value was hardcoded to 100.
- Grafana dashboards on the "Monitor" tab of the Management Console are better labeled and organized.
  - Dashboards include a "[collectd]" or "[OpenTelemetry]" prefix based on their monitoring stack.

  - The "External MySQL" dashboard is hidden unless External MySQL is enabled.
  - OpenTelemetry dashboards have the "opentelemetry" tag, not the "prometheus" tag.

- To limit misleading error messages when the `mysql_exporter` and `sql_exporter` exporters try to connect to the database, both exporters use an IPv4 address.
- On an instance with busy databases, online schema migrations using gh-ost failed because the cut-over lock timeout defaulted to 3 seconds, which was insufficient to acquire an exclusive table lock under continuous traffic.
- When creating a new organization, members who already have access through enterprise teams are no longer listed individually on the invite page. A banner is shown instead, with a link to manage enterprise team access.
- To improve page load performance, user profile pages display a maximum of 24 organizations. When viewing your own profile, a "View all" link provides access to the full list in organization settings. When viewing another users profile, a count displays any additional organizations beyond the first 24.

3.20.1: Known issues

- First time setups of GitHub Actions with OpenID Connect (OIDC) fail with an error on the `Update Servicing Resources` step. This problem does not affect instances where GitHub Actions is already enabled.

  As a workaround, you can enable Actions without OIDC, then enable OIDC **immediately** once the process completes. You should do this immediately because enabling OIDC will remove all access to existing Actions logs and artifacts.
- During an upgrade of GitHub Enterprise Server, custom firewall rules are removed. If you use custom firewall rules, you must reapply them after upgrading.
- 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.

- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.
- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- When restoring data originally backed up from a 3.13 or greater appliance version, the Elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- After a restore, existing outside collaborators cannot be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version

and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

- When applying an enterprise security configuration to all repositories (for example, enabling Secret Scanning or Code Scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.
- In GHES instances that have multiple git storage nodes in a voting configurations (That includes GHES Clusters and Geo Replicate HA instances) where Actions is enabled can encounter problem a upon upgrading. The 1st part actions that are shipped with the new version of GHES can not be correctly installed. This can block upgrade and in some cases leave the old versions of these actions within the instatance.

Enterprise Server 3.20.0

Download GitHub Enterprise Server 3.20.0

March 17, 2026

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

3.20.0: Features

- **Instance administration**
  - You can configure a dedicated disk for log storage, mounted at `/var/log` and configured as an LVM volume, to isolate logs from the root disk. This capability is in public preview and applies only to standalone and high availability topologies. It does not apply to cluster topologies. See Configuring multiple data disks.

  - The backup service, previously in public preview, is now generally available in GitHub Enterprise Server 3.20. The managed, built-in service provides an alternative to GitHub Enterprise Server backup utilities and does not require a separate host for backup software. See About the backup service for GitHub Enterprise Server. Please note that Backup Utilities will be retired starting in version 3.22.

  - You can add additional nodes to a high-availability datacenter to offload CPU-intensive tasks from the primary data node, allowing horizontal scaling for GitHub Enterprise Server. This capability is in public preview and applies only to high-availability topologies. It does not apply to standalone or to cluster topologies. See Adding nodes to a high availability configuration.

- **Identity and access management**

  - Enterprise owners can create and manage enterprise teams to simplify governance across their enterprise. Using the API or enterprise settings UI, owners can assign enterprise teams to organizations, create and assign custom enterprise roles, and assign roles to both teams and users. Organization and repository owners can assign roles to enterprise teams within their scope, and enterprise teams can be added to ruleset bypass lists. There are product limitations to this experience. This feature is in public preview and subject to change. See Teams in an enterprise.

- **GitHub Connect**

  - Site administrators can enable GitHub Connect to resolve open source actions from GitHub.com, even when their GHES instance is connected to a data-resident enterprise on GHE.com. This enables hybrid deployment scenarios during migration to GHE.com. This feature is in public preview and subject to change.

- **Code scanning**

  - Administrators can enable code scanning using default setup even if an organization or repository's GitHub Actions policies would otherwise prevent uploading Actions workflows. This change allows security scans to proceed without being blocked by policy controls on Actions. See Enforcing policies for GitHub Actions in your enterprise.

  - GitHub Advanced Security customers can track and manage security remediation work by assigning code scanning alerts to themselves or other users. This feature is in public preview and subject to change.

- This release comes installed with version 2.23.9 of the CodeQL CLI, used in the CodeQL action for code scanning. Significant updates since the default version installed on GitHub Enterprise Server 3.19 include:
  - Users can now analyze Rust projects using CodeQL, with Rust support now generally available. Developers working on Rust libraries and apps can benefit from code security analysis covering all OWASP Top 10 categories (except A06:2021-Vulnerable and Outdated Components).
  - Users can enable CodeQL on C/C++ repositories more easily, as scanning C/C++ projects without builds is now generally available. Default setup uses build-mode none for all newly configured repositories, significantly helping improve ease of adoption.
  - CodeQL now supports incremental analysis of all supported languages, helping improve analysis performance.
  - Users of code scanning advanced setup need to update their workflow files to use CodeQL Action v4, which runs on the Node.js 24 runtime. Users of default setup will automatically move to v4 without taking action. CodeQL Action v3 will be closing down in December 2026. Read more on the GitHub blog.
  - Users working with Swift can analyze projects using Swift 6.2 and 6.2.1, with CodeQL now supporting these versions.
  - Users analyzing Kotlin codebases can scan projects built with Kotlin 2.2.0x and 2.2.2x, as CodeQL adds support for these new releases. Support for Kotlin 1.6 and 1.7 has been closed down and will be removed in CodeQL 2.24.1.
  - There have also been a variety of improvements and changes to CodeQL queries across all languages
  - Read more in the changelogs for the CodeQL versions included in this release:
    - CodeQL 2.23.0
    - CodeQL 2.23.1
    - CodeQL 2.23.2
    - CodeQL 2.23.3
    - CodeQL 2.23.4
    - CodeQL 2.23.5
    - CodeQL 2.23.6
    - CodeQL 2.23.7 and 2.23.8

- **Secret scanning**
  - Secret scanning supports alert assignees, including webhook events and REST API endpoints to view and update assignees for triage workflows.

  - Secret scanning adds new detectors and improves detectors for existing secret types, expanding coverage and improving accuracy for detected secrets. See Supported secret scanning patterns.
  - Secret scanning supports validity checks that indicate whether detected secrets remain active, helping teams prioritize remediation. Once enabled for a given repository, GitHub will now automatically verify secrets for alerts with supported secret types. GHES admins can make the feature available for enablement across enterprise repositories from their Management Console settings.
  - Secret scanning push protection expands default coverage to block additional secrets, reducing the risk of credential leaks during pushes.
  - Enterprise owners can configure delegated bypass for secret scanning push protection at the enterprise level, and reviewers can manage bypass requests from the enterprise.

- **GitHub Advanced Security**
  - The Enterprise Security Manager role is available on GitHub Enterprise Server to manage security policies and view alerts across an enterprise. The role is supported only for enterprises with up to 15,000 organizations. This feature is in public preview.

- **Dependabot**
  - Organizations can specify custom runner labels for Dependabot jobs on self-hosted runners.
  - Dependabot now supports version updates for Conda packages.

- **GitHub Actions**
  - For self-hosted GitHub Actions runners on this GitHub Enterprise Server release, the minimum required version of the GitHub Actions Runner application is 2.330.0. See the release notes for this version in the `actions/runner` repository. If your instance uses ephemeral self-hosted runners and you've disabled automatic updates, you must upgrade your runners to this version of the Runner application before upgrading your instance to this GitHub Enterprise Server release.
  - Users who trigger workflows manually or via API can use up to 25 inputs on workflows triggered via the `workflow_dispatch` trigger. This is an increase from the previous limit of 10 inputs.

  - Users who configure reusable workflows in GitHub Actions can nest up to 10 reusable workflows and call up to 50 workflows in total from a given workflow run, an increase from the previous limits of 4 nested workflows and 20 total workflows.
  - Site administrators can enhance security for public repositories using self-hosted runners. GitHub Actions validates both the pull request author and the event Actor before determining whether workflows should run for pull request events originating from forked repositories. See the GitHub blog and Managing GitHub Actions settings for a repository.
  - In the web UI for GitHub Actions, workflow runs display relative timestamps for the first day after a run starts, then switch to absolute date and time. This makes it easier to confirm when a run occurred without hovering.

- **Community experience**
  - The notification counter in the sidebar accurately reflects the number of notifications, excluding any that have been marked as spam and removed. Previously, the counter incorrectly included spam notifications even after removal.

- **Organizations**
  - Organization owners and moderators can review blocked users in organization settings with more context, including when a user was blocked and who performed the action. The blocked user description limit is higher to support detailed rationale and URLs for auditing and accountability.
  - Organization owners can prevent repository administrators from installing GitHub Apps. By default, repository administrators can install apps that don't require organization-level permissions. This setting restricts app installation to organization owners only, improving security and compliance governance.

- **Projects**
  - You can use the Projects GraphQL API to track additional events, such as status changes, when items are added or removed from a project, and conversions from drafts to issues. Filtering project items using a project filter is also now available. See the GitHub blog.
  - GitHub Projects has an improved onboarding flow that helps users import items from a repository, choose a default repository, and find templates and views more easily. These improvements reduce setup time and help users get started faster.

- **Pull requests**
  - The improved merge experience from pull requests pages includes UX enhancements and integration of repository rules. It's now easier to convert pull requests to draft status from the merge box, monitor failing optional status checks, and remove pull requests from the merge queue.

- **Releases**
  - Releases support immutability, locking release assets from being added, modified, or deleted after publication. The release tag cannot be moved, and cannot be deleted while the release exists. If the release is deleted, the tag can be removed but cannot be reused. This helps protect distributed artifacts from supply chain attacks. Release attestations are not supported on GHES and are only available on GitHub.com.

3.20.0: Changes

- To support GitHub Enterprise Server compatibility, we're reserving the `/repos` path for a forthcoming product feature. If you currently use `/repos` for a route (for example, a User name, Organization name, a GitHub App, OAuth app, reverse proxy, or internal integration), you may need to update your configuration to avoid routing conflicts. This change ensures consistent behavior for GHES 3.20 customers and helps prevent unexpected request handling for endpoints under `/repos`.

3.20.0: Known issues

- Custom firewall rules are removed during the upgrade process.
- 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. See Troubleshooting access to the Management Console.
- In some situations, large `.adoc` files stored in a repository do not render properly in the web UI. The raw contents are still available to view as plaintext.

- Admin stats REST API endpoints may timeout on appliances with many users or repositories. Retrying the request until data is returned is advised.
- When following the steps for Replacing the primary MySQL node, step 14 (running `ghe-cluster-config-apply`) might fail with errors. If this occurs, re-running `ghe-cluster-config-apply` is expected to succeed.
- Running a config apply as part of the steps for Replacing a node in an emergency may fail with errors if the node being replaced is still reachable. If this occurs, shutdown the node and repeat the steps.
- When restoring data originally backed up from a 3.13 or greater appliance version, the elasticsearch indices need to be reindexed before some of the data will show up. This happens via a nightly scheduled job. It can also be forced by running `/usr/local/share/enterprise/ghe-es-search-repair`.
- When initializing a new GHES cluster, nodes with the `consul-server` role should be added to the cluster before adding additional nodes. Adding all nodes simultaneously creates a race condition between nomad server registration and nomad client registration.
- Admins setting up cluster high availability (HA) may encounter a spokes error when running `ghe-cluster-repl-status` if a new organization and repositories are created before using the `ghe-cluster-repl-bootstrap` command. To avoid this issue, complete the cluster HA setup with `ghe-cluster-repl-bootstrap` before creating new organizations and repositories.
- In a cluster, the host running restore requires access the storage nodes via their private IPs.
- On an instance hosted on Azure, commenting on an issue via email meant the comment was not added to the issue.
- After a restore, existing outside collaborators are unable to be added to repositories in a new organization. This issue can be resolved by running `/usr/local/share/enterprise/ghe-es-search-repair` on the appliance.
- After a geo-replica is promoted to be a primary by running `ghe-repl-promote`, the actions workflow of a repository does not have any suggested workflows.
- When publishing npm packages in a workflow after restoring from a backup to GitHub Enterprise Server 3.13.5.gm4 or 3.14.2.gm3, you may encounter a `401 Unauthorized` error from the GitHub Packages service. This can happen if the restore is from an N-1 or N-2 version and the workflow targets the npm endpoint on the backup instance. To avoid this issue, ensure the access token is valid and includes the correct scopes for publishing to GitHub Packages.

- When applying an enterprise security configuration to all repositories (for example, enabling Secret Scanning or Code Scanning across all repositories), the system immediately enqueues enablement jobs for every organization in the enterprise simultaneously. For enterprises with a large number of repositories, this can result in significant system load and potential performance degradation. If you manage a large enterprise with many organizations and repositories, we recommend applying security configurations at the organization level rather than at the enterprise level in the UI. This allows you to enable security features incrementally and monitor system performance as you roll out changes.

- When viewing the status of an ongoing backup on the "Backups" page of the Management Console, the backup may initially report as "incomplete" instead of "in progress". You can ignore the initial "incomplete" status because the backup is still running and will report the correct status once it has progressed further. In some configurations, such as cluster topologies, this may take up to 5 minutes.

- GHES instances that have multiple Git storage nodes in a voting configurations (including GHES Clusters and Geo Replicate HA instances) where Actions is enabled can encounter a problem upon upgrading. Part of Actions that are shipped with the new version of GHES can not be correctly installed. This can block upgrades and in some cases leave the old versions of these Actions within the instance. If this occurs running the following command on the primary node should help correct the problem: `ghe-config --unset 'app.actions.actions-repos-sha1sum' /usr/local/share/enterprise/ghe-run-init-actions-graph`

3.20.0: Closing down

- The `first`, `last`, and `page` parameters for offset-based pagination are closing down in the REST API endpoints for listing Dependabot alerts at the repository, organization, and enterprise levels. Use cursor-based pagination with the `before`, `after`, and `per_page` parameters instead.

- High availability replication for cluster topologies will be retired starting in GitHub Enterprise Server 3.22. You will no longer be able to configure or use the feature, and we will remove the supporting code from the product.

- Notifications generated from @mentions in commit messages will be removed in a future release. This change will help users focus on more relevant notifications and reduce overall notification load, as feedback from maintainers has shown these notifications are rarely useful.

Legal

© 2026 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog