Jenkins Security Advisory 2025-04-02

This advisory announces vulnerabilities in the following Jenkins deliverables:

- Jenkins (core)
- AsakusaSatellite Plugin
- Cadence vManager Plugin
- monitor-remote-job Plugin
- Simple Queue Plugin
- Stack Hammer Plugin
- Templating Engine Plugin

Descriptions

Missing permission check allows retrieving agent configurations

SECURITY-3512 / CVE-2025-31720
Severity (CVSS): Medium
Description:

Jenkins 2.503 and earlier, LTS 2.492.2 and earlier does not perform a permission check in an HTTP endpoint.

This allows attackers with Agent/Create permission but without Agent/Extended Read permission to copy an agent, gaining access to its configuration.

Jenkins 2.504, LTS 2.492.3 requires Agent/Extended Read permission to copy an agent.

Missing permission check allows retrieving secrets from agent configurations

SECURITY-3513 / CVE-2025-31721
Severity (CVSS): Medium
Description:

Jenkins 2.503 and earlier, LTS 2.492.2 and earlier does not perform a permission check in an HTTP endpoint.

This allows attackers with Agent/Create permission but without Agent/Configure permission to copy an agent, gaining access to encrypted secrets in its configuration.

This is due to an incomplete fix of SECURITY-3495.

Jenkins 2.504, LTS 2.492.3 requires Agent/Configure permission to copy an agent containing secrets.

Script Security sandbox bypass vulnerability through folder-scoped libraries in Templating Engine Plugin

SECURITY-3505 / CVE-2025-31722
Severity (CVSS): High
Affected plugin: `templating-engine`
Description:

Templating Engine Plugin allows defining libraries both in the global configuration, as well as scoped to folders containing the pipelines using them. While libraries in the global configuration can only be set up by administrators and can therefore be trusted, libraries defined in folders can be configured by users with Item/Configure permission.

In Templating Engine Plugin 2.5.3 and earlier, libraries defined in folders are not subject to sandbox protection. This vulnerability allows attackers with Item/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM.

In Templating Engine Plugin 2.5.4, libraries defined in folders are subject to sandbox protection.

CSRF vulnerability in Simple Queue Plugin

SECURITY-3469 / CVE-2025-31723

Severity (CVSS): Medium
Affected plugin: `simple-queue`
Description:

Simple Queue Plugin 1.4.6 and earlier does not require POST requests for multiple HTTP endpoints, resulting in cross-site request forgery (CSRF) vulnerabilities.

These vulnerabilities allow attackers to change and reset the build queue order.

Simple Queue Plugin 1.4.7 requires POST requests for the affected HTTP endpoints.

> Administrators can enable equivalent HTTP endpoints without CSRF protection via the global configuration.

API keys stored in plain text by Cadence vManager Plugin

SECURITY-3537 / CVE-2025-31724
Severity (CVSS): Medium
Affected plugin: `vmanager-plugin`
Description:

Cadence vManager Plugin 4.0.0-282.v5096a_c2db_275 and earlier stores Verisium Manager vAPI keys unencrypted in job `config.xml` files on the Jenkins controller as part of its configuration.

These API keys can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.

Cadence vManager Plugin 4.0.1-286.v9e25a_740b_a_48 stores Verisium Manager vAPI keys encrypted once affected job configurations are saved again.

Passwords stored in plain text by monitor-remote-job Plugin

SECURITY-3539 / CVE-2025-31725
Severity (CVSS): Medium
Affected plugin: `monitor-remote-job`
Description:

monitor-remote-job Plugin 1.0 stores passwords unencrypted in job `config.xml` files on the Jenkins controller as part of its configuration.

These passwords can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.

As of publication of this advisory, there is no fix. Learn why we announce this.

API keys stored in plain text by Stack Hammer Plugin

SECURITY-3520 / CVE-2025-31726
Severity (CVSS): Medium
Affected plugin: `stackhammer`
Description:

Stack Hammer Plugin 1.0.6 and earlier stores Stack Hammer API keys unencrypted in job `config.xml` files on the Jenkins controller as part of its configuration.

These API keys can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.

As of publication of this advisory, there is no fix. Learn why we announce this.

API keys stored and displayed in plain text by AsakusaSatellite Plugin

SECURITY-3523 / CVE-2025-31727 (storage), CVE-2025-31728 (masking)
Severity (CVSS): Medium
Affected plugin: `asakusa-satellite-plugin`
Description:

AsakusaSatellite Plugin 0.1.1 and earlier stores AsakusaSatellite API keys unencrypted in job `config.xml` files on the Jenkins controller as part of its configuration.

These API keys can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.

Additionally, the job configuration form does not mask these API keys, increasing the potential for attackers to observe and capture them.

As of publication of this advisory, there is no fix. Learn why we announce this.

Severity

- SECURITY-3469: Medium
- SECURITY-3505: High
- SECURITY-3512: Medium
- SECURITY-3513: Medium
- SECURITY-3520: Medium
- SECURITY-3523: Medium
- SECURITY-3537: Medium
- SECURITY-3539: Medium

Affected Versions

- **Jenkins weekly** up to and including 2.503
- **Jenkins LTS** up to and including 2.492.2
- **AsakusaSatellite Plugin** up to and including 0.1.1
- **Cadence vManager Plugin** up to and including 4.0.0-282.v5096a_c2db_275
- **monitor-remote-job Plugin** up to and including 1.0
- **Simple Queue Plugin** up to and including 1.4.6
- **Stack Hammer Plugin** up to and including 1.0.6
- **Templating Engine Plugin** up to and including 2.5.3

Fix

- **Jenkins weekly** should be updated to version 2.504
- **Jenkins LTS** should be updated to version 2.492.3
- **Cadence vManager Plugin** should be updated to version 4.0.1-286.v9e25a_740b_a_48
- **Simple Queue Plugin** should be updated to version 1.4.7
- **Templating Engine Plugin** should be updated to version 2.5.4

These versions include fixes to the vulnerabilities described above. All prior versions are considered to be affected by these vulnerabilities unless otherwise indicated.

As of publication of this advisory, no fixes are available for the following plugins:

- AsakusaSatellite Plugin
- monitor-remote-job Plugin
- Stack Hammer Plugin

Learn why we announce these issues.

Credit

The Jenkins project would like to thank the reporters for discovering and reporting these vulnerabilities:

- **Daniel Beck, CloudBees, Inc.** for SECURITY-3512, SECURITY-3513
- **Romuald Moisan, Aix Marseille University, and Vincent Lardet, Aix Marseille University** for SECURITY-3523, SECURITY-3537
- **Swapna Nanda, CloudBees, Inc.** for SECURITY-3469
- **Zaoui Zakariae, Aix Marseille University** for SECURITY-3539
- **Zaoui Zakariae, Aix Marseille University, and Romuald Moisan, Aix Marseille University** for SECURITY-3520

⚠ Report an Infra Issue

Improve this page

⚠ Report page issue

Resources

Downloads
Blog
Documentation

Plugins
Security
Contributing

Project

Structure and governance
Issue tracker
Roadmap
GitHub
Jenkins on Jenkins
Statistics

Community

Forum
Events
Mailing lists
Chats
Special Interest Groups
𝕏 (formerly Twitter)
Reddit

Other

Code of Conduct
Press information
Merchandise
Artwork
Awards