Jenkins Security Advisory 2024-11-13

This advisory announces vulnerabilities in the following Jenkins deliverables:

- Authorize Project Plugin
- IvyTrigger Plugin
- OpenId Connect Authentication Plugin
- Pipeline: Declarative Plugin
- Pipeline: Groovy Plugin
- Script Security Plugin
- Shared Library Version Override Plugin

Descriptions

Missing permission check in Script Security Plugin

SECURITY-3447 / CVE-2024-52549
Severity (CVSS): Medium
Affected plugin: `script-security`
Description:

Script Security Plugin 1367.vdf2fc45f229c and earlier, except 1365.1367.va_3b_b_89f8a_95b_ and 1362.1364.v4cf2dc5d8776, does not perform a permission check in a method implementing form validation.

This allows attackers with Overall/Read permission to check for the existence of files on the controller file system.

Script Security Plugin 1368.vb_b_402e3547e7 requires Overall/Administer permission for the affected form validation method.

Rebuilding a run with revoked script approval allowed by Pipeline: Groovy Plugin

SECURITY-3362 / CVE-2024-52550
Severity (CVSS): High
Affected plugin: `workflow-cps`
Description:

Pipeline: Groovy Plugin 3990.vd281dd77a_388 and earlier, except 3975.3977.v478dd9e956c3, does not check whether the main (Jenkinsfile) script for a rebuilt build is approved.

This allows attackers with Item/Build permission to rebuild a previous build whose (Jenkinsfile) script is no longer approved.

This does not apply to builds whose (Jenkinsfile) script was never approved, but only to builds whose (Jenkinsfile) script got its approval revoked.

Pipeline: Groovy Plugin 3993.v3e20a_37282f8 refuses to rebuild a build whose main (Jenkinsfile) script is unapproved.

Restarting a run with revoked script approval allowed by Pipeline: Declarative Plugin

SECURITY-3361 / CVE-2024-52551
Severity (CVSS): High
Affected plugin: `pipeline-model-definition`
Description:

Pipeline: Declarative Plugin 2.2214.vb_b_34b_2ea_9b_83 and earlier does not check whether the main (Jenkinsfile) script used to restart a build from a specific stage is approved.

This allows attackers with Item/Build permission to restart a previous build whose (Jenkinsfile) script is no longer approved.

This does not apply to builds whose (Jenkinsfile) script was never approved, but only to builds whose (Jenkinsfile) script got its approval revoked.

Pipeline: Declarative Plugin 2.2218.v56d0cda_37c72 refuses to restart a build whose main (Jenkinsfile) script is unapproved.

Stored XSS vulnerability in Authorize Project Plugin

SECURITY-3010 / CVE-2024-52552
Severity (CVSS): High
Affected plugin: `authorize-project`
Description:

Authorize Project Plugin 1.7.2 and earlier evaluates a string containing the job name with JavaScript on the Authorization view.

This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.

Authorize Project Plugin 1.8.0 no longer evaluates a string containing the job name with JavaScript on the Authorization view.

Session fixation vulnerability in OpenId Connect Authentication Plugin

SECURITY-3473 / CVE-2024-52553
Severity (CVSS): High

Affected plugin: `oic-auth`
Description:

OpenId Connect Authentication Plugin 4.418.vccc7061f5b_6d and earlier does not invalidate the existing session on login.

This allows attackers to use social engineering techniques to gain administrator access to Jenkins.

OpenId Connect Authentication Plugin 4.421.v5422614eb_e0a_ invalidates the existing session on login.

XXE vulnerability in IvyTrigger Plugin

SECURITY-2954 / CVE-2022-46751
Severity (CVSS): High
Affected plugin: `ivytrigger`
Description:

IvyTrigger Plugin 1.01 and earlier bundles versions of Apache Ivy vulnerable to CVE-2022-46751.

This allows attackers able to control the input files for the "IvyTrigger - Poll with an Ivy script" build trigger to have Jenkins parse a crafted XML document that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.

IvyTrigger Plugin 1.02 updates the bundled Apache Ivy version to 2.5.2, which is unaffected by this issue.

Script security bypass vulnerability in Shared Library Version Override Plugin

SECURITY-3466 / CVE-2024-52554
Severity (CVSS): High
Affected plugin: `shared-library-version-override`
Description:

Shared Library Version Override Plugin 17.v786074c9fce7 and earlier declares folder-scoped library overrides as trusted, so that they’re not executed in the Script Security sandbox.

This allows attackers with Item/Configure permission on a folder to configure a folder-scoped library override that runs without sandbox protection.

Shared Library Version Override Plugin 19.v3a_c975738d4a_ declares folder-scoped library overrides as untrusted, so that they’re executed in the Script Security sandbox.

Severity

- SECURITY-2954: High
- SECURITY-3010: High
- SECURITY-3361: High
- SECURITY-3362: High
- SECURITY-3447: Medium
- SECURITY-3466: High
- SECURITY-3473: High

Affected Versions

- **Authorize Project Plugin** up to and including 1.7.2
- **IvyTrigger Plugin** up to and including 1.01
- **OpenId Connect Authentication Plugin** up to and including 4.418.vccc7061f5b_6d
- **Pipeline: Declarative Plugin** up to and including 2.2214.vb_b_34b_2ea_9b_83
- **Pipeline: Groovy Plugin** up to and including 3990.vd281dd77a_388

- **Script Security Plugin** up to and including 1367.vdf2fc45f229c
- **Shared Library Version Override Plugin** up to and including 17.v786074c9fce7

Fix

- **Authorize Project Plugin** should be updated to version 1.8.0
- **IvyTrigger Plugin** should be updated to version 1.02
- **OpenId Connect Authentication Plugin** should be updated to version 4.421.v5422614eb_e0a_
- **Pipeline: Declarative Plugin** should be updated to version 2.2218.v56d0cda_37c72
- **Pipeline: Groovy Plugin** should be updated to version 3993.v3e20a_37282f8
- **Script Security Plugin** should be updated to version 1368.vb_b_402e3547e7
- **Shared Library Version Override Plugin** should be updated to version 19.v3a_c975738d4a_

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

Credit

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

- **Daniel Beck, CloudBees, Inc.** for SECURITY-3466
- **Kevin Guerroudj, CloudBees, Inc.** for SECURITY-3010, SECURITY-3361, SECURITY-3362, SECURITY-3473