مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Jenkins Plugins

Tracking #:432319193

Date:25-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in several Jenkins plugins. The issues include sandbox bypass, command injection, CSRF flaws, permission bypass, information disclosure, and remote code execution risks. Some affected plugins currently have no available fixes.

TECHNICAL DETAILS:

Vulnerability Details

High Severity

- CVE-2026-57280 — Sandbox bypass vulnerability in Script Security Plugin
- CVE-2026-57281 — Script security bypass vulnerability in Script Security Plugin
- CVE-2026-57296 — Path traversal vulnerability in External Workspace Manager Plugin
- CVE-2026-57301 — Builds executed on the Jenkins controller by OWASP ZAP Plugin can lead to RCE
- CVE-2026-57303 — XXE vulnerability in Assembla Plugin

Medium Severity

- CVE-2026-57282 — OS command injection vulnerability on agents in Git client Plugin
- CVE-2026-57283 — CSRF vulnerability in Pipeline: Groovy Plugin
- CVE-2026-57284 — Unrestricted instantiation of types in Pipeline: Groovy Plugin
- CVE-2026-57285 — Missing permission check allows enumerating GitHub Enterprise server URLs in GitHub Branch Source Plugin
- CVE-2026-57286 — Missing permission check in Git Parameter Plugin allows listing SCM branch and tag names
- CVE-2026-57287 — Encrypted values of secrets in job and agent configurations not redacted by Job Configuration History Plugin
- CVE-2026-57300 — Missing permission check in MCP Server Plugin allows reading Pipeline replay scripts
- CVE-2026-57289 — SSL/TLS certificate validation unconditionally disabled by Bitbucket Push and Pull Request Plugin
- CVE-2026-57290 — CSRF vulnerability in Priority Sorter Plugin
- CVE-2026-57291 — Missing permission check in Gitee Plugin
- CVE-2026-57292 — CSRF vulnerability in Gitee Plugin
- CVE-2026-57293 — Incorrect permission check in Gitee Plugin allows enumerating credentials IDs
- CVE-2026-57294 — Missing permission check in EC2 Fleet Plugin
- CVE-2026-57295 — CSRF vulnerability in EC2 Fleet Plugin
- CVE-2026-57297 — Missing permission check in Contrast Continuous Application Security Plugin
- CVE-2026-57298 — CSRF vulnerability in Contrast Continuous Application Security Plugin
- CVE-2026-57299 — Missing permission checks in Contrast Continuous Application Security Plugin allow enumerating Contrast metadata
- CVE-2026-57302 — Passwords stored in plain text by FitNesse Plugin
- CVE-2026-57304 — Missing permission check in Assembla Plugin
- CVE-2026-57305 — CSRF vulnerability in Assembla Plugin
- CVE-2026-57306 — CSRF vulnerability in Zowe zDevOps Plugin
- CVE-2026-57307 — Missing permission check in Zowe zDevOps Plugin

Low Severity

- CVE-2026-57288 — LDAP injection vulnerability in Active Directory Plugin

Successful exploitation could allow attackers to execute code on Jenkins controllers or agents, access sensitive credentials, or bypass authentication and authorization mechanisms. Several affected plugins currently have no available fixes, increasing overall risk to Jenkins environments.

Affected Versions

- Active Directory Plugin up to and including 2.41.1
- Assembla Plugin up to and including 1.4
- Bitbucket Push and Pull Request Plugin up to and including 3.3.8
- Contrast Continuous Application Security Plugin up to and including 3.11
- EC2 Fleet Plugin up to and including 4.2.3.539.v8fedff2a_81c3
- External Workspace Manager Plugin up to and including 1.3.2
- FitNesse Plugin up to and including 1.36
- Git client Plugin up to and including 6.6.0
- Git Parameter Plugin up to and including 462.vdcf3df2ed2ca_
- Gitee Plugin up to and including 1288.v18b_deb_c9069b_
- GitHub Branch Source Plugin up to and including 1967.1969.v205fd594c821
- Job Configuration History Plugin up to and including 1356.ve360da_6c523a_
- MCP Server Plugin up to and including 0.177.v629fdb_2557fe
- OWASP ZAP Plugin up to and including 1.0.7
- Pipeline: Groovy Plugin up to and including 4331.v9d06ed4658ff
- Priority Sorter Plugin up to and including 936.v2c01c6b_84449
- Script Security Plugin up to and including 1402.v94c9ce464861
- Zowe zDevOps Plugin up to and including 1.1.3.50.ve350c9b_450b_1

Fixed Versions

- Active Directory Plugin → 2.41.2
- Bitbucket Push and Pull Request Plugin → 3.3.9
- Contrast Continuous Application Security Plugin → 3.12
- EC2 Fleet Plugin → 4.2.3.540.va_6eedb_7b_c112
- External Workspace Manager Plugin → 1.4.0
- Git Client Plugin → 6.6.1
- Git Parameter Plugin → 462.463.v496a_59f698e5
- Gitee Plugin → 1292.v2559f2f3f2c0
- GitHub Branch Source Plugin → 1967.1970.vd86979736546
- Job Configuration History Plugin → 1367.vc8fa_b_15101dc
- MCP Server Plugin → 0.178.vffe5a_e770f3b_
- Pipeline: Groovy Plugin → 4331.4333.v50a_b_076c5199
- Priority Sorter Plugin → 936.937.v5581d0b_2ccb_a_
- Script Security Plugin → 1402.1405.vc96e74964250

No fixes available yet for:

- Assembla Plugin
- FitNesse Plugin
- OWASP ZAP Plugin
- Zowe zDevOps Plugin

RECOMMENDATIONS:

- Keep Jenkins and all plugins updated with the latest security fixes.

- For plugins without available fixes, monitor vendor advisories and apply updates as soon as they are released.
- Remove or disable unused or unpatched plugins.
- Enforce least privilege access and strong role-based controls.
- Restrict access to Jenkins admin and controller interfaces.
- Limit and review script execution and sandbox exceptions.
- Monitor logs for unusual pipeline or plugin activity.
- Ensure TLS is properly enforced for all external integrations.
- Regularly audit plugins, configurations, and stored credentials.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.jenkins.io/security/advisory/2026-06-24/