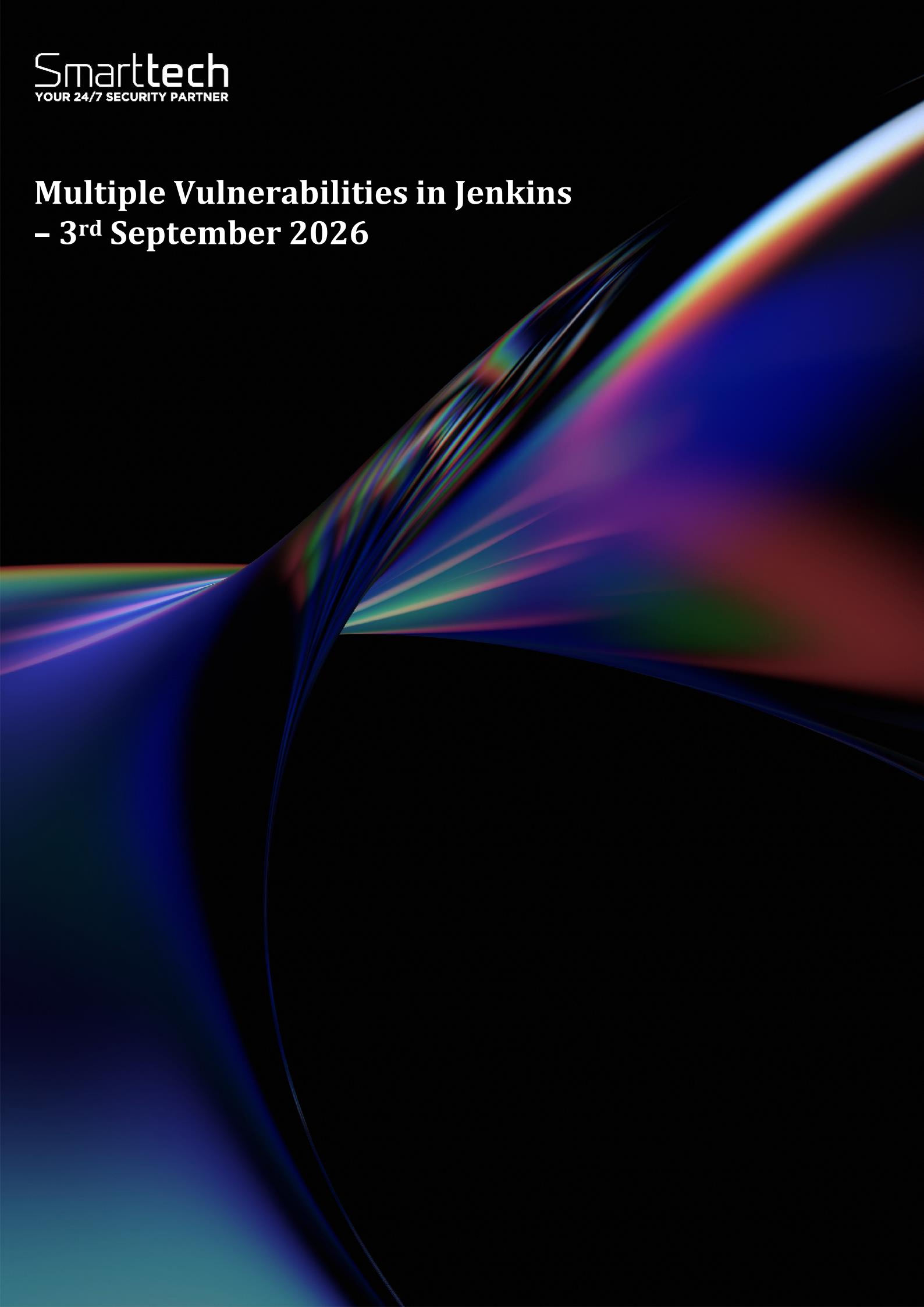
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Jenkins – 3rd September 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	151
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-03
Issue Date	2026-09-03

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple vulnerabilities have been identified in Jenkins. Successful exploitation could result in arbitrary code execution, unauthorized access, privilege escalation, information disclosure, and cross-site request forgery.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	***Description***
Deserialization vulnerability **CVE-2026-84645** CVSS Base Score: 8.8	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, objects of types marked as storing their configuration in independent top-level configuration files in Jenkins (such as the global configuration and jobs) can appear as nested field values in user-submitted `config.xml` documents and subsequently handle HTTP requests via Stapler, resulting in remote code execution.
Lack of type restriction in deserialization allows creating user objects **CVE-2026-84646** CVSS Base Score: 4.3	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, user objects can appear as nested field values in other deserialized XML objects, allowing attackers with Overall/Read permission to create user objects by submitting crafted XML.
Instantiation of any types related to configuration **CVE-2026-84647** CVSS Base Score: **8.8**	In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Stapler does not restrict the types of objects that can be instantiated via form data binding to those compatible with the expected field type, allowing attackers with Overall/Read permission to instantiate types related to configuration for which that field type was not intended.

Stored XSS vulnerability in system log viewer **CVE-2026-84648** CVSS Base Score: 8.8	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the system log viewer does not escape log record metadata (source, level, and timestamp) resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers in control of agent processes.
Cross-origin exposure of CSRF token **CVE-2026-70430** CVSS Base Score: **2.7**	In Stapler 1839.ved17667b_a_eb_5 through 2107.v8dfcb_e8ed317 (both inclusive), except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.447 through 2.579 (both inclusive), LTS 2.452.1 through 2.568.2 (both inclusive), an HTTP endpoint serving dynamically generated JavaScript resources embeds the user's cross-site request forgery (CSRF) token (crumb) as a string literal, allowing attackers with control over a page hosted on the same site as Jenkins to obtain a valid crumb for the targeted user's session and perform actions on their behalf.
Unsafe deserialization allows overwriting configuration objects **CVE-2026-84650** CVSS Base Score: **8.8**	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, transient fields cannot be excluded from deserialization, allowing attackers able to submit configuration updates to specify the values of transient fields that will be deserialized, the impact depending on how those fields are used.
Unsafe deserialization allows overwriting other agents **CVE-2026-84651** CVSS Base Score: **6.3**	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the REST API and CLI endpoints for updating agent configuration do not prevent a submitted configuration from overwriting a different agent by specifying that agent's name in the submitted XML document, allowing attackers with Agent/Configure permission on one agent to take over a different agent, gaining control of its configuration and obtaining access to its inbound agent secret and environment variables.
Session fixation vulnerability **CVE-2026-84652** CVSS Base Score: **7.5**	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Jenkins does not rotate the session when a user is authenticated via the "remember me" cookie, allowing attackers able to serve content on the same site as Jenkins to set a known session cookie in the victim's browser, which after the victim authenticates via the "remember me" cookie, grants the attacker access to Jenkins as that user.
Incorrect permission check in Appearance configuration page **CVE-2026-84653** CVSS Base Score: **6.8**	Jenkins 2.421 through 2.579 (both inclusive), LTS 2.426.1 through 2.568.2 (both inclusive) does not correctly perform permission checks in the Appearance configuration page, allowing attackers with Overall/Manage permission to modify Appearance configuration options they should not have access to.
Form submission data binding can set static fields **CVE-2026-84654** CVSS Base Score: **5.4**	In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, form data binding allows setting public static fields of the bound configuration object, allowing attackers who can submit configuration forms to modify public static fields of the configuration objects those forms are bound to, resulting in changes that apply globally to the Jenkins instance.

Injection vulnerability in REST API **CVE-2026-84655** CVSS Base Score: **4.3**	Jenkins 2.579 and earlier, LTS 2.568.2 and earlier does not escape map keys when serializing objects as JSON and Python through its REST API, allowing attackers able to control map property names to inject arbitrary fields into JSON and Python API responses.
Missing permission check allows reading build parameters **CVE-2026-84656** CVSS Base Score: **4.3**	A missing permission check in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier allows attackers with Item/Read permission on at least one job to read build parameter names and values of jobs they have no access to.
Missing permission check allows canceling builds **CVE-2026-84657** CVSS Base Score: **4.2**	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the build CLI command does not check the Item/Cancel permission when using the -s flag to cancel a build triggered to wait for completion, allowing attackers with Item/Build permission to cancel builds started by other users.
Improper access control in Script Security Plugin **CVE-2026-84658 (script approval),** **CVE-2026-84659 (Groovy sandbox)** CVSS Base Score: **4.3**	Jenkins Script Security Plugin 1412.v7737b_3405f86 and earlier uses the `@DataBoundConstructor` annotation on a constructor that loads script approval configuration, allowing attackers able to submit certain forms to read that configuration. Jenkins Script Security Plugin 1412.v7737b_3405f86 and earlier does not enforce a permission check in the method that controls the "Force the use of the sandbox globally in the system" setting, allowing attackers to disable it through Stapler data binding.
Missing permission check in Pipeline: Build Step Plugin allows canceling downstream builds **CVE-2026-84660 (build step),** **CVE-2026-84661 (waitForBuild step)** CVSS Base Score: **5.4**	A missing permission check in Jenkins Pipeline: Build Step Plugin 599.v4b_67ea_11b_152 and earlier causes downstream builds triggered by the `build` step to be canceled even when the build's authentication lacks Item/Cancel permission on the downstream job. A missing permission check in Jenkins Pipeline: Build Step Plugin 599.v4b_67ea_11b_152 and earlier causes downstream builds awaited by the `waitForBuild` step when the `propagateAbort` parameter is used to be canceled even when the build's authentication lacks Item/Cancel permission on the downstream job.
Improper access control in LDAP Plugin allows SSRF **CVE-2026-84662** CVSS Base Score: **4.3**	Jenkins LDAP Plugin 807.809.vd3a_4e5e4ec98 and earlier allows connecting to a specified URL through Stapler data binding, allowing attackers to connect to an attacker-specified URL.
CSRF vulnerability in Pipeline: Groovy Libraries Plugin **CVE-2026-84663** CVSS Base Score: **5.4**	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline: Groovy Libraries Plugin 798.v5cc688825312 and earlier allows attackers to delete shared library caches.
Improper access control in GitLab Plugin allows SSRF **CVE-2026-84664** CVSS Base Score: **5.4**	Jenkins GitLab Plugin 1.9.16 and earlier allows overwriting the global GitLab connection configuration through Stapler data binding, allowing attackers to connect to an attacker-specified URL using GitLab API tokens already configured by administrators.

Stored XSS vulnerability in SonarQube Scanner Plugin **CVE-2026-84665** CVSS Base Score: **8**	Jenkins SonarQube Scanner Plugin 2.18.3 and earlier does not limit URL schemes for the dashboard links it creates based on SonarQube scanner results, allowing the `javascript:` scheme, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.
Improper access control in Job Configuration History Plugin **CVE-2026-84666** CVSS Base Score: **5.4**	Jenkins Job Configuration History Plugin 1367.vc8fa_b_15101dc and earlier allows overwriting the plugin's history recording configuration through Stapler data binding, allowing attackers to redirect history storage to an attacker-specified directory and modify history recording settings.
Improper access control in ThinBackup Plugin **CVE-2026-84667** CVSS Base Score: **7.1**	Jenkins ThinBackup Plugin 2.1.4 and earlier allows overwriting the plugin's backup configuration through Stapler data binding, allowing attackers to redirect backup writes to an attacker-specified directory and to include arbitrary files from the Jenkins controller file system in backups.
Improper access control in SAML Plugin **CVE-2026-84668** CVSS Base Score: **8.8**	Jenkins SAML Plugin 4.618.v441a_27fa_46d2 and earlier allows overwriting the SAML identity provider metadata file through Stapler data binding, allowing attackers to replace it with attacker-controlled content and authenticate as any user.
Path traversal vulnerability in Allure Plugin **CVE-2026-84669** CVSS Base Score: **8.8**	A path traversal vulnerability in Jenkins Allure Plugin 2.35.2 and earlier allows attackers with Item/Read permission on jobs that publish Allure report results to read arbitrary files on the Jenkins controller's file system.
Deserialization of untrusted data vulnerability in Performance Plugin **CVE-2026-84670** CVSS Base Score: **8.8**	Jenkins Performance Plugin 1015.v09ca_52b_3370e and earlier does not restrict the classes that can be instantiated when deserializing cached performance reports stored in the build directory on the Jenkins controller, allowing attackers with Item/Configure permission to execute arbitrary code on the Jenkins controller.
Path traversal vulnerability in File Parameter Plugin can lead to RCE **CVE-2026-84671** CVSS Base Score: **8.8**	Jenkins File Parameter Plugin 425.v3fa_801681b_5e and earlier allows writing files to arbitrary locations on the Jenkins controller file system through Stapler data binding, which can lead to remote code execution.
Privilege escalation in Microsoft Entra ID (previously Azure AD) Plugin **CVE-2026-84672** CVSS Base Score: **8.8**	Jenkins Microsoft Entra ID (previously Azure AD) Plugin 710.v0b_ff8e9cc2d2 and earlier grants Entra group permissions using both the group's unique object ID and its display name, allowing attackers who can create an Entra group with a colliding display name to gain the permissions configured for a privileged group.
Improper access control in Customizable Header Plugin leads to XSS **CVE-2026-84673** CVSS Base Score: **8.8**	Jenkins Customizable Header Plugin 295.v2544b_ca_19b_97 and earlier allows overwriting the plugin's appearance configuration through Stapler data binding, allowing attackers to configure a custom SVG icon containing inline JavaScript, resulting in a stored cross-site scripting (XSS) vulnerability.

Missing permission checks in XebiaLabs XL Deploy Plugin allow enumerating credentials IDs **CVE-2026-84674** CVSS Base Score: **5.4**	Missing permission checks in Jenkins XebiaLabs XL Deploy Plugin 26.1.0 and earlier allow attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.
OS command injection vulnerability on agents in TICS Plugin **CVE-2026-84675** CVSS Base Score: **7.4**	OS command injection vulnerability in Jenkins TICS Plugin 2025.1.1 and earlier allows attackers able to control build environment variable values to execute arbitrary commands on the agent running the build.
Tokens stored in plain text by Parameterized Remote Trigger Plugin **CVE-2026-84676** CVSS Base Score: **4.3**	Jenkins Parameterized Remote Trigger Plugin 3.2.2 and earlier stores tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.
Stored XSS vulnerability in update-center2 **CVE-2026-84677** CVSS Base Score: **5.4**	Jenkins update-center2 3.18.3 and earlier does not escape plugin-provided values (plugin names, descriptions, and version metadata) on plugin download index pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a plugin for hosting.

Affected Products:

- Jenkins weekly up to and including 2.579
- Jenkins LTS up to and including 2.568.2
- Allure Plugin up to and including 2.35.2
- Customizable Header Plugin up to and including 295.v2544b_ca_19b_97
- File Parameter Plugin up to and including 425.v3fa_801681b_5e
- GitLab Plugin up to and including 1.9.16
- Job Configuration History Plugin up to and including 1367.vc8fa_b_15101dc
- LDAP Plugin up to and including 807.809.vd3a_4e5e4ec98
- Microsoft Entra ID (previously Azure AD) Plugin up to and including 710.v0b_ff8e9cc2d2
- Parameterized Remote Trigger Plugin up to and including 3.2.2
- Performance Plugin up to and including 1015.v09ca_52b_3370e
- Pipeline: Build Step Plugin up to and including 599.v4b_67ea_11b_152
- Pipeline: Groovy Libraries Plugin up to and including 798.v5cc688825312
- SAML Plugin up to and including 4.618.v441a_27fa_46d2
- Script Security Plugin up to and including 1412.v7737b_3405f86
- SonarQube Scanner Plugin up to and including 2.18.3
- ThinBackup Plugin up to and including 2.1.4
- TICS Plugin up to and including 2025.1.1
- XebiaLabs XL Deploy Plugin up to and including 26.1.0
- update-center2 up to and including 3.18.3

Fixed Versions:

- Jenkins weekly up to and including 2.579
- Jenkins LTS up to and including 2.568.2
- Allure Plugin up to and including 2.35.2
- Customizable Header Plugin up to and including 295.v2544b_ca_19b_97
- File Parameter Plugin up to and including 425.v3fa_801681b_5e
- GitLab Plugin up to and including 1.9.16
- Job Configuration History Plugin up to and including 1367.vc8fa_b_15101dc

- LDAP Plugin up to and including 807.809.vd3a_4e5e4ec98
- Microsoft Entra ID (previously Azure AD) Plugin up to and including 710.v0b_ff8e9cc2d2
- Parameterized Remote Trigger Plugin up to and including 3.2.2
- Performance Plugin up to and including 1015.v09ca_52b_3370e
- Pipeline: Build Step Plugin up to and including 599.v4b_67ea_11b_152
- Pipeline: Groovy Libraries Plugin up to and including 798.v5cc688825312
- SAML Plugin up to and including 4.618.v441a_27fa_46d2
- Script Security Plugin up to and including 1412.v7737b_3405f86
- SonarQube Scanner Plugin up to and including 2.18.3
- ThinBackup Plugin up to and including 2.1.4
- TICS Plugin up to and including 2025.1.1
- XebiaLabs XL Deploy Plugin up to and including 26.1.0
- update-center2 up to and including 3.18.3

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

- Parameterized Remote Trigger Plugin

Recommendations

Smarttech247 team recommend the following actions to be taken:

- Apply appropriate updates provided by Jenkins to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
    - Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - Safeguard 7.2: Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - Safeguard 7.4: Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - Safeguard 7.7: Remediate Detected Vulnerabilities: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - Safeguard 18.1: Establish and Maintain a Penetration Testing Program: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable

hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - Safeguard 18.2: Perform Periodic External Penetration Tests: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - Safeguard 18.3: Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (M1016: Vulnerability Scanning)
    - Safeguard 16.13: Conduct Application Penetration Testing: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (M1026: Privileged Account Management)
    - Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
    - Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently
- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (M1030: Network Segmentation)
    - Safeguard 12.2: Establish and Maintain a Secure Network Architecture: Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050: Exploit Protection)
    - Safeguard 10.5: Enable Anti-Exploitation Features: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (M1021: Restrict Web-Based Content)

    - Safeguard 9.2: Use DNS Filtering Services: Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - Safeguard 9.3: Maintain and Enforce Network-Based URL Filters: Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - Safeguard 9.6: Block Unnecessary File Types: Block unnecessary file types attempting to enter the enterprise's email gateway.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. (M1017: User Training)
    - Safeguard 14.1: Establish and Maintain a Security Awareness Program: Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks: Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

References

https://www.jenkins.io/security/advisory/2026-09-02/

CVEs

CVE-2026-84645,
CVE-2026-84646,
CVE-2026-84647,
CVE-2026-84648,
CVE-2026-84649,
CVE-2026-84650,
CVE-2026-84651,
CVE-2026-84652,
CVE-2026-84653,
CVE-2026-84654,
CVE-2026-84655,
CVE-2026-84656,
CVE-2026-84657,
CVE-2026-84658,
CVE-2026-84659,
CVE-2026-84660,
CVE-2026-84661,
CVE-2026-84662,
CVE-2026-84663,
CVE-2026-84664,
CVE-2026-84665,
CVE-2026-84666,
CVE-2026-84667,
CVE-2026-84668,
CVE-2026-84669,
CVE-2026-84670,
CVE-2026-84671,
CVE-2026-84672,
CVE-2026-84673,
CVE-2026-84674,
CVE-2026-84675,
CVE-2026-84676,
CVE-2026-84677


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com