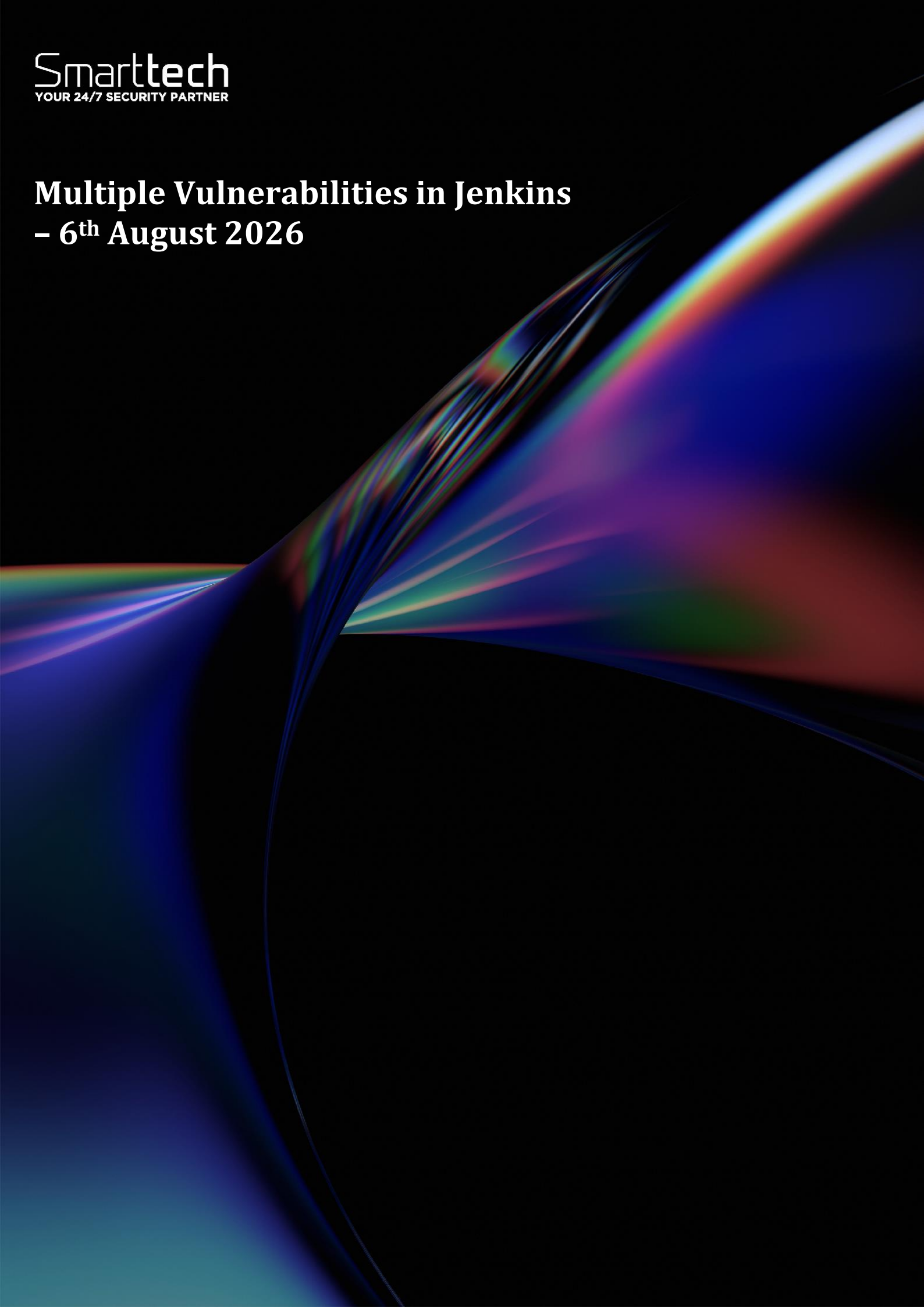
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Jenkins – 6th August 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	129
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-06
Issue Date	2026-08-05

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***
Agent-to-controller deserialization filter bypass **CVE-2026-70426** CVSS Base Score: **9.0**	Jenkins uses the Remoting library (typically agent.jar or remoting.jar) for communication between the controller and agents via serialized Java objects. To protect against deserialization vulnerabilities, Jenkins enforces the JEP-200 class filter during deserialization of objects received over a Remoting channel on the controller. In Remoting 3384.v60d89463d9e0 and earlier, except 3355.3357.v931d3c992987, included in Jenkins 2.575 and earlier, LTS 2.568.1 and earlier, the JEP-200 class filter is not applied to classes resolved via a fallback path in the Remoting deserialization implementation. This allows agent processes, code running on agents, and attackers with Agent/Connect permission to bypass the JEP-200 deserialization filter for classes on the Jenkins core classpath, which could be leveraged to execute code on the Jenkins controller. This is limited to classes on the Jenkins core classpath (i.e., bundled with Jenkins or part of the Java platform) that are not on the pre-JEP-200 deserialization denylist. Dependencies bundled with plugins will not be deserialized. The Remoting library in Jenkins 2.576,

	LTS 2.568.2 also applies the class filter on the fallback code path.
Link following vulnerability allows arbitrary file creation **CVE-2026-70427** CVSS Base Score: **8.8**	Jenkins 2.575 and earlier, LTS 2.568.1 and earlier does not safely handle symbolic links with effectively empty names during the extraction of .tar and .tar.gz archives. This allows attackers able to control agent processes to provide crafted archives to the controller to write files to arbitrary locations on the file system, restricted only by file system access permissions of the user running Jenkins. This can result in code execution by, e.g., writing malicious scripts to the JENKINS_HOME/init.groovy.d/ directory (feature documentation), or deploying plugins to JENKINS_HOME/plugins/. Jenkins 2.576, LTS 2.568.2 refuses to extract files from .tar and .tar.gz archives that contain symbolic links with effectively empty names.
Path traversal vulnerability in file parameters **CVE-2026-70428** CVSS Base Score: **8.8**	Jenkins 2.575 and earlier, LTS 2.568.1 and earlier improperly identifies file paths attempting path traversal in file parameter names. This allows attackers with Item/Configure and Item/Build permission to write files to arbitrary locations on the controller file system, restricted only by file system access permissions of the user running Jenkins. This can result in code execution by, e.g., writing malicious scripts to the JENKINS_HOME/init.groovy.d/ directory (feature documentation), or deploying plugins to JENKINS_HOME/plugins/. Jenkins 2.576, LTS 2.568.2 improves the identification of file paths attempting path traversal in file parameter names, preventing writing files to arbitrary locations on the file system.
Improper handling of case sensitivity allows privilege escalation **CVE-2026-70429** CVSS Base Score: 8.1	Jenkins 2.575 and earlier, LTS 2.568.1 and earlier handles case-insensitivity in user names and group names inconsistently. While the canonical ID for a case-insensitive user or group name is created by lowercasing the name, comparisons of user names and group names are done using String#equalsIgnoreCase. The latter considers some Unicode characters to be equal to other characters, while the former does not (e.g., the letter "dotless i" ı being equal to regular lowercase i). This allows attackers able to create new users or groups with names that case-insensitively match other characters to impersonate other users or be granted their permissions. This requires a security realm that allows these characters in user names or group names, and allows creation of users or groups that case-insensitively match existing users or groups. The Jenkins user database does not allow users to sign up with usernames outside of the ASCII range. Jenkins 2.576, LTS 2.568.2 compares usernames and group names using their canonical form and only considers them equal if their canonical forms are equal.

Users with Overall/Manage permission can instantiate any types related to configuration **CVE-2026-70430** CVSS Base Score: **2.7**	Jenkins 2.575 and earlier, LTS 2.568.1 and earlier does not restrict the types of objects that can be instantiated as part of the project naming strategy configuration. This allows attackers with Overall/Manage permission to instantiate arbitrary types related to configuration, including those intended for configuration only by administrators. Jenkins 2.576, LTS 2.568.2 restricts the types of objects that can be instantiated as part of the project naming strategy configuration to those related to that feature.
Arbitrary code execution vulnerability in Multijob Plugin **CVE-2026-70431** CVSS Base Score: **8.8**	Multijob Plugin 669.v9d96a_d9c71b_0 and earlier provides Groovy scripting features that do not integrate with Script Security Plugin. This vulnerability allows attackers with Item/Create or Item/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM. Multijob Plugin 677.v7ffc23d6a_4c2 integrates with Script Security Plugin to enforce sandboxing of Groovy scripts.
CSRF vulnerability in Multijob Plugin allows arbitrary code execution **CVE-2026-70432** CVSS Base Score: **8.8**	Multijob Plugin 669.v9d96a_d9c71b_0 and earlier does not require POST requests for a form validation endpoint, resulting in a cross-site request forgery (CSRF) vulnerability. This vulnerability allows attackers to execute arbitrary code in the context of the Jenkins controller JVM. Multijob Plugin 677.v7ffc23d6a_4c2 requires POST requests for the affected form validation endpoint.
Missing permission checks in HCL AppScan Plugin allow enumerating credentials IDs **CVE-2026-70433** CVSS Base Score: **4.3**	HCL AppScan Plugin 1.8.3 and earlier does not perform permission checks in multiple HTTP endpoints. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. HCL AppScan Plugin 1.8.4 requires appropriate permissions in the affected HTTP endpoints.
CSRF vulnerability and missing permission checks in SCM-Manager Plugin **CVE-2026-70434 (CSRF)** **CVE-2026-70435 (permission check)** CVSS Base Score: **4.2**	SCM-Manager Plugin 1.11.1 and earlier does not perform permission checks in several HTTP endpoints. This allows attackers with Overall/Read permission to connect to an attacker-specified HTTP URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. Additionally, these endpoints do not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability. SCM-Manager Plugin 1.12.1 requires POST requests and Item/Configure permission for these endpoints.
Missing permission check in External Workspace Manager Plugin allows reading workspace files **CVE-2026-70436** CVSS Base Score: **4.3**	External Workspace Manager Plugin 1.4.1 and earlier does not perform a permission check (1.4.0 and earlier) or performs an improper permission check (1.4.1) when providing access to externally-managed workspaces through the workspace browser. This allows attackers with Overall/Read permission to read files in workspaces they are not authorized to access. External Workspace Manager Plugin 1.4.2 performs the expected permission check

	before providing access to externally-managed workspaces through the workspace browser.
Non-constant time webhook bearer token comparison in Webhook Secret Credentials Provider Plugin **CVE-2026-70437** CVSS Base Score: **3.7**	Webhook Secret Credentials Provider Plugin 16.v0cfa_f0215cf5 and earlier does not use a constant-time comparison function when checking whether the provided and expected webhook bearer token are equal. This could potentially allow attackers to use statistical methods to obtain a valid webhook bearer token. Webhook Secret Credentials Provider Plugin 32.v09c9b_522f0a_8 uses a constant-time comparison when validating the webhook bearer token.
Missing permission checks in Parameterized Remote Trigger Plugin allow enumerating credentials IDs **CVE-2026-70438** CVSS Base Score: **4.3**	Parameterized Remote Trigger Plugin 3.2.2 and earlier does not perform permission checks in HTTP endpoints. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. As of publication of this advisory, there is no fix.
Missing permission checks in XML Job to Job DSL Plugin **CVE-2026-70439** CVSS Base Score: **6.5**	XML Job to Job DSL Plugin 0.1.13 and earlier does not perform permission checks, and makes its functionality available to users lacking Overall/Read permission. While only jobs the user has Item/Read permission for will be accessible, it does not require Item/Extended Read permission to convert their configuration. Additionally, the plugin allows any user to invoke the conversion functionality, replacing any previously generated output in userContent. As of publication of this advisory, there is no fix.
Stored XSS vulnerability in Qualys Container Scanning Connector Plugin **CVE-2026-70440** CVSS Base Score: **8.0**	Qualys Container Scanning Connector Plugin 1.8.0.5 and earlier does not escape user-controlled field values in a JavaScript context. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. As of publication of this advisory, there is no fix.
Stored XSS vulnerability in Summary Display Plugin **CVE-2026-70441** CVSS Base Score: **8.0**	Summary Display Plugin 1.15 and earlier does not escape the job name in a JavaScript context in build report pages. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Create or Item/Configure permission. As of publication of this advisory, there is no fix.
Exposure of System-scoped credentials in Google Chat Notification Plugin **CVE-2026-70442** CVSS Base Score: **4.3**	Google Chat Notification Plugin 166.ve6b_de280f2e8 and earlier does not set the appropriate context for credentials lookup, allowing the use of System-scoped credentials otherwise reserved for the global configuration. This allows attackers with Item/Configure permission to access and capture credentials they are not entitled to use. As of publication of this advisory, there is no fix.
Exposure of System-scoped credentials in Horreum Plugin **CVE-2026-70443** CVSS Base Score: **4.3**	Horreum Plugin 0.16.162.v33b_4a_a_b_5f828 and earlier does not set the appropriate context for credentials lookup, allowing the use of System-scoped credentials otherwise reserved for the global configuration. This allows attackers with

	Item/Configure permission to have Jenkins send credentials they are not entitled to use to the administrator-configured Horreum URL. As of publication of this advisory, there is no fix.
Missing permission check in Violation Comments to GitLab Plugin allows enumerating credentials IDs **CVE-2026-70444** CVSS Base Score: **4.3**	Violation Comments to GitLab Plugin 2.62.0 and earlier does not perform a permission check in an HTTP endpoint. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. As of publication of this advisory, there is no fix.
Missing permission checks in Sauce OnDemand Plugin allow enumerating credentials IDs **CVE-2026-70445** CVSS Base Score: **4.3**	Sauce OnDemand Plugin 2.2.0 and earlier does not perform permission checks in several HTTP endpoints. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. As of publication of this advisory, there is no fix.
Missing permission checks in CodeSonar Plugin allow enumerating credentials IDs **CVE-2026-70446** CVSS Base Score: **4.3**	CodeSonar Plugin 3.6.0 and earlier does not perform permission checks in several HTTP endpoints. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. As of publication of this advisory, there is no fix.
Missing permission checks in AWS CodeBuild Plugin allow enumerating credentials IDs **CVE-2026-70447** CVSS Base Score: **4.3**	AWS CodeBuild Plugin 0.59 and earlier does not perform permission checks in several HTTP endpoints. This allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. Those can be used as part of an attack to capture the credentials using another vulnerability. As of publication of this advisory, there is no fix.
XXE vulnerability in Ivy Report Plugin **CVE-2026-70448** CVSS Base Score: **7.1**	Ivy Report Plugin 1.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. This allows attackers able to control workspace contents to have Jenkins parse a crafted Ivy report XML file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery. As of publication of this advisory, there is no fix.

Affected Products:

- Jenkins weekly up to and including 2.575
- Jenkins LTS up to and including 2.568.1
- AWS CodeBuild Plugin up to and including 0.59
- CodeSonar Plugin up to and including 3.6.0
- External Workspace Manager Plugin up to and including 1.4.1
- Google Chat Notification Plugin up to and including 166.ve6b_de280f2e8
- HCL AppScan Plugin up to and including 1.8.3
- Horreum Plugin up to and including 0.16.162.v33b_4a_a_b_5f828
- Ivy Report Plugin up to and including 1.2
- Multijob Plugin up to and including 669.v9d96a_d9c71b_0

- Parameterized Remote Trigger Plugin up to and including 3.2.2
- Qualys Container Scanning Connector Plugin up to and including 1.8.0.5
- Sauce OnDemand Plugin up to and including 2.2.0
- SCM-Manager Plugin up to and including 1.11.1
- Summary Display Plugin up to and including 1.15
- Violation Comments to GitLab Plugin up to and including 2.62.0
- Webhook Secret Credentials Provider Plugin up to and including 16.v0cfa_f0215cf5
- XML Job to Job DSL Plugin up to and including 0.1.13

Fixed Versions:

- Jenkins weekly should be updated to version 2.576
- Jenkins LTS should be updated to version 2.568.2
- External Workspace Manager Plugin should be updated to version 1.4.2
- HCL AppScan Plugin should be updated to version 1.8.4
- Multijob Plugin should be updated to version 677.v7ffc23d6a_4c2
- SCM-Manager Plugin should be updated to version 1.12.1
- Webhook Secret Credentials Provider Plugin should be updated to version 32.v09c9b_522f0a_8

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

- AWS CodeBuild Plugin
- CodeSonar Plugin
- Google Chat Notification Plugin
- Horreum Plugin
- Ivy Report Plugin
- Parameterized Remote Trigger Plugin
- Qualys Container Scanning Connector Plugin
- Sauce OnDemand Plugin
- Summary Display Plugin
- Violation Comments to GitLab Plugin
- XML Job to Job DSL 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/2026-08-05/

CVEs

CVE-2026-70426
CVE-2026-70427

CVE-2026-70428
CVE-2026-70429
CVE-2026-70430
CVE-2026-70431
CVE-2026-70432
CVE-2026-70433
CVE-2026-70434
CVE-2026-70435
CVE-2026-70436
CVE-2026-70437
CVE-2026-70438
CVE-2026-70439
CVE-2026-70440
CVE-2026-70441
CVE-2026-70442
CVE-2026-70443
CVE-2026-70444
CVE-2026-70445
CVE-2026-70446
CVE-2026-70447
CVE-2026-70448


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