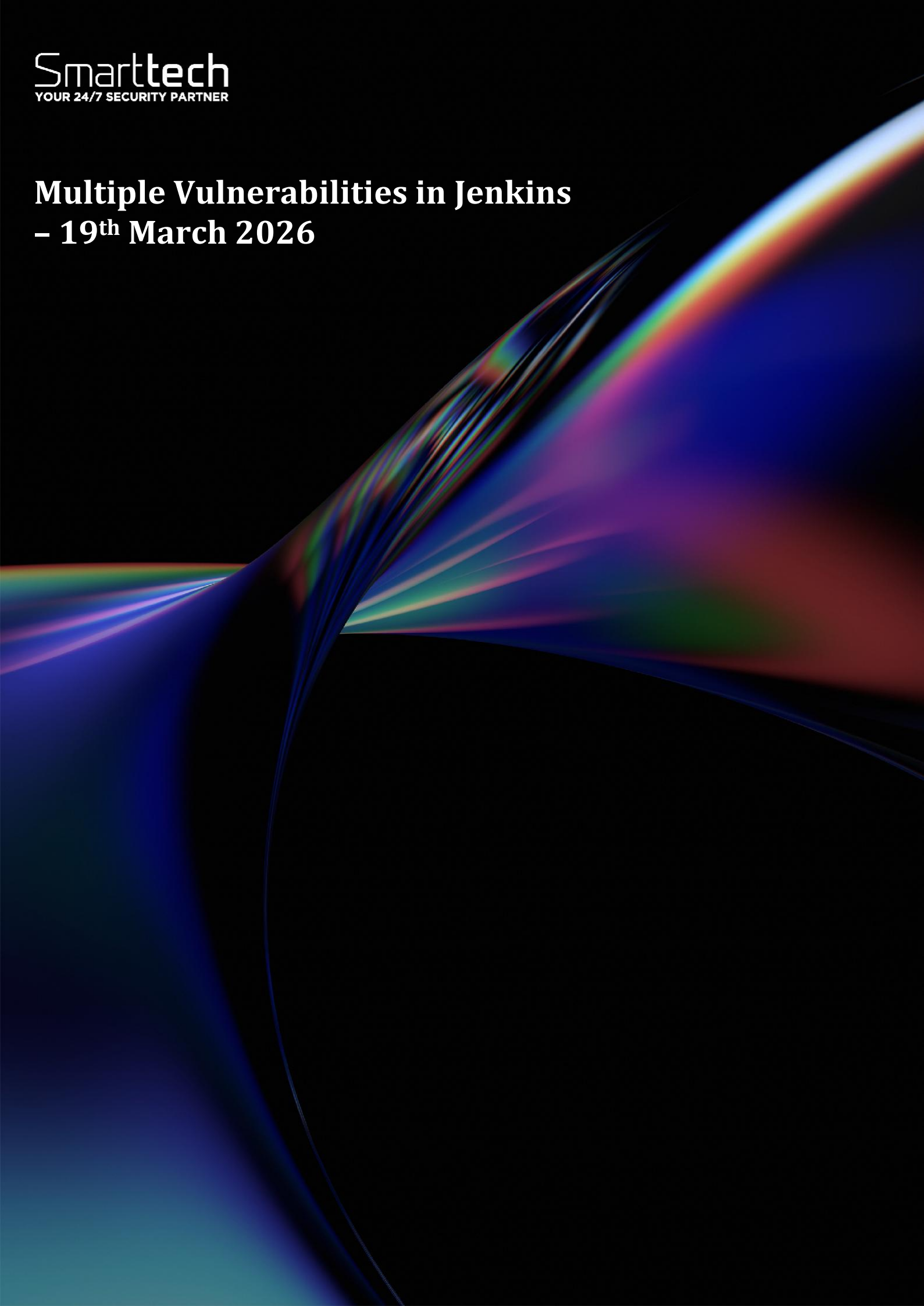
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Jenkins – 19th March 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	38
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-03-19
Issue Date	2026-03-19

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, affecting versions up to and including 2.554, LTS releases up to and including 2.541.2 and LoadNinja Plugin up to and including 2.1. Successful exploitation could allow for arbitrary code execution, authentication bypass, information disclosure, unauthorized access, and CLI command execution.

Risk

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	***Description***
Link following vulnerability allows arbitrary file creation **CVE-2026-33001** CVSS Base Score: **8.8**	Jenkins 2.554 and earlier, LTS 2.541.2 and earlier does not safely handle symbolic links during the extraction of .tar and .tar.gz archives. This allows crafted archives to write files to arbitrary locations on the filesystem, restricted only by file system access permissions of the user running Jenkins. For archives extracted on the controller, this can result in code execution by, e.g., writing malicious scripts to the JENKINS_HOME/init.groovy.d/ directory, or deploying plugins to JENKINS_HOME/plugins/.
DNS rebinding vulnerability in WebSocket CLI origin validation **CVE-2026-33002** CVSS Base Score: **7.5**	Jenkins has a built-in command line interface (CLI) to access Jenkins from a script or shell environment. Since Jenkins 2.217 and LTS 2.222.1, one of the ways to communicate with the CLI is through a WebSocket endpoint. Jenkins 2.442 through 2.554 (both inclusive), LTS 2.426.3 through LTS 2.541.2 (both inclusive) performs this origin validation by computing the expected origin for comparison

	using the Host or X-Forwarded-Host HTTP request headers. This allows attackers to bypass the origin validation using DNS rebinding attacks. By causing a victim to visit a malicious website that uses DNS rebinding to resolve to the Jenkins controller's IP address, attackers can establish a WebSocket connection to the CLI endpoint from an untrusted origin and execute CLI commands as the anonymous user.
API keys stored and displayed in plain text by LoadNinja Plugin **CVE-2026-33003 (storage)** **CVE-2026-33004 (masking)** CVSS Base Score: **4.3**	LoadNinja Plugin 2.1 and earlier stores LoadNinja 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.

Affected Products:

- Jenkins weekly up to and including 2.554
- Jenkins LTS up to and including 2.541.2
- LoadNinja Plugin up to and including 2.1

Fixed Versions:

- Jenkins weekly should be updated to version 2.555
- Jenkins LTS should be updated to version 2.541.3
- LoadNinja Plugin should be updated to version 2.2

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/2026-03-18/

CVEs

CVE-2026-33001
CVE-2026-33002
CVE-2026-33003
CVE-2026-33004

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com