Threat Intelligence and CVE Analysis Report

Toan Tran

CPSC 253

Prof. Franklin

December 13, 2024

**Introduction**

In the cyber world, where threats and vulnerabilities happen daily, threat intelligence should be a priority because it signals that organizations must seek solutions to improve defensive barriers to defend against attacks. Threat intelligence also allows the organization to respond quickly to mitigate risks on assets and outline insights and analyses about threat actors or hackers and their intentions, thereby assisting the organization's decision-making and risk monitoring and management (Franklin, 2024). The CVE analysis is significant because it notifies people about publicity vulnerabilities and their exploited techniques. The list provides measurements on severity level for organizations to release security patches. Based on the CVE list, organizations remeasure the security flaws in their tools and weaknesses in regulation procedures and fix them to protect availability, integrity, and confidentiality (Tungal, 2024).

**CVE Research Details**

This selected CVE is associated with Jenkins, an open-source server designed for developers to produce, evaluate, and deploy software. Their recent security advisory has been published concerning the critical vulnerability that exploited the Jenkins files via their remote code interfaces. The National Vulnerability Database has classified this vulnerability as CVE-23897, with a 9.8 CVSS score, pointing to a highly critical risk, and revealed to the public on January 24, 2024 (NIST, 2024). With a high CVSS score, this unpleasant incident violated all integrity, availability, and confidentiality. According to the official website Jenkins report, vulnerability emerged when Jenkins decided to “use the args4j library to parse the command arguments and options on the Jenkins controller during processing command line interface (CLI),” and the CLI tool misinterpreted the file directory starting with prefix @ (Jenkins Security Advisory, 2024). These details denote the shift in functionality within the file path with the

prefix @ and directly launched and retrieved secret data within that file’s subjects (expandAtFiles), the util library failed to achieve its purpose and provided a backdoor for attackers. Those attackers steal sensitive data within the Jenkins file controller system by taking advantage of files with standard character encoding weaknesses. However, it must be based on the strict assumption of knowledge about the target path, or else the attack plan can terminate at the initial step for the sake of time and resources. The impact level of the incident depends on attackers meeting basic requirements like meeting the correct path on how many details attackers obtain from those files, which violates the access control and increases attack surfaces; notably, attackers explore the whole file with overall/read permission. Unfortunately, even those without authentication and no pre-install plugins can also sneakily read the first few lines. However, with prerequisite requirements, according to Yaniv Nizry, the author of “Excessive Expansion: Uncovering Critical Security Vulnerabilities in Jenkins, “[claims] the signed-up feature is enabled. Legacy mode authorization is enabled. Configuration ‘allow anonymous read access’ is checked in the ‘logged-in users can do anything’ authorization mode” (Nizry, 2024).

Aside from remote code execution, this vulnerability also allowed users to skip over security constraints, unauthorized access and theft of data, and cross-site scripting (Jenkins Security Advisory, 2024). After eluding the security restriction, threat actors can break in and turn off defensive features, becoming wide open to the next attack wave. Attackers with cross-site scripting can access victim accounts after tricking users into filling out login identifications on malicious websites or corrupting whole pages with malware and viruses. Those impacts cause data and personal info leaks, damage organizations' virtual assets, and insider top secrets.

This CVE introduces various attack vectors that are caused by remote code execution through "resources root URL variant 1 and 2, 'Remember me' cookie, CSRF protection bypass,

and stored cross-site scripting (XSS)" and several ways to access, steal asset and identity and corrupt files, server around website "decrypt secrets, delete any item, download a Java heap dump" (Jenkins Security Advisory, 2024). This attack list once again recalled the importance of threat intelligence, the knowledge of CVE, and other defensive techniques. Among those attack vectors, remote code execution through Resource Root URL variant 1 is potentially the most severe case that quickly targets. The exploitation can only be achieved when users turn on the resources' root URL configuration feature or the wrong reverse proxy. For instance, it is common for basic-level developers to use command lines to access their files and built-in tools without mind because of the security approach, mainly because they do not edit those default features. That is why it is still risky because enabling that feature because it checked by default on outdated version, allows anonymous unauthenticated attackers to gain direct access to the CLI WebSocket endpoint (Jetty) and predict usernames and passwords through the arbitrary files with overall/read consent "on native installers, packages, or on Docker containers or when running Jenkins with the command java -jar jenkins.war" (Jenkins Security Advisory, 2024). Multiple consequences are uncovered depending on which exploited methods and how their configuration is set up. After successfully analyzing those binary files, attackers can take control of that specific file system with the following consequences: injecting malicious stuff like malware and payload with CLI, taking over ownership and stealing user credentials, stealing cryptographic keys to crack other sensitive things (if possible). The Jenkins 2.441 and earlier versions are directly affected by this vulnerability. According to Jenkin' statistics, Windows is more likely to get exploited than Linux with UTF-8 encoding because there are only a few illegally encoded symbols (5 out of 256), so attackers have a higher chance of correctly predicting the symbols (Jenkins Security

Advisory, 2024). The possible solution for this incident is upgrading to the latest version; however, if users do not want to corrupt their work or want to keep the older version, they can turn off the command line interface as a temporary approach to prevent prohibited access.

**Event Analysis**

Because real-life cyber threats happen here and there, attack techniques become more diverse and evolve to the point that it becomes common for threat actors to break attacks on infrastructure frameworks and harm assets. In the article, "Ransomware attack on Indian payment system traced back to Jenkins bug," Jonathan Greig (2024) specified this selected event where threat actors abused Jenkins vulnerability to indirectly damage the National Payments Corporation of India (NPCI) on July 31, 2024. To be more precise, the RansomEXX threat team corrupted C-Edge Technologies, a third-party provider, by executing ransomware on CLI to outdated Jenkins servers used within their company. During the offline period, NPCI quarantined C-Edge Technologies and blocked all their customers from using digital payment services. C-Edge Technologies successfully brought back their business in a brief period. Sadly, the same gang had stolen 142 GB of digital payment data during the second strike (Greig, 2024).

As the summary mentioned above, CVE-2024-23897 has a relationship with the events regarding misconception and failure management. The C-edge Technologies should have known the Jenkins version back in January, checking patches were released a while ago, and the CVE and NDA also warned against the potential risks correlated to vulnerabilities. Nevertheless, whether C-edge Technologies disregards this warning or does not know about the issue is still being determined. They are the ones who should be claimed for this falsely because they could have been safe from exploitation if they had managed every security patch with proper care. Another relationship between them is the misconfiguration of older Jenkins patches. After

placing the @ prefix in front of the file path that is an entrance, the CLI parse code is unable to diagnose, which gives the RansomExx team the freedom to send ransomware to intrude the sensitive payment data files and grab related information stored on the open-source server, and disrupting the NPCI operating and networking system, causing numerous failure services to banks across India nation.

This attack on C-edge company emphasizes the urgent need for scanning and checking patch updates regularly, and do update, do not ignore it. This event is a wake-up call for all organizations to continue to train and practice awareness for their employees to limit regrettable moments. For example, organizations with strict server configurations, network monitoring, and managing policies and frameworks could minimize exploitation risks. Also, the primary organization must constantly check to ensure that the third-party company is maintained correctly and create a transparency and accountability contract and standard, doing so the primary organization to prevent constant failure. With experience from this event, organizations must enhance their backup and comprehensive incident response plan. Although the third-party company resolves downtime is not long, they should take additional measures to isolate all ransomware to no network connection with multiple-layer protection virtual machines and turn off CLI features to limit the potential of the attack surface. With this procedure, this third-party company should be able to prevent the second strike, not just recover backup service without turning off Jenkins vulnerable features and affected system. Companies should also adopt advantage detection and prevent intrusion, strengthen their security system with extra layers, set up a correct reverse proxy, conduct regular audits, and implement limited access control and good security practices for reserve information systems.

These events follow with multiple potential risks, including financial, operational, reputational, network, and legal risks. The financial and reputational risk is represented by the RansomEXX team stealing valuable payment information that causes a loss of trust in the company and valuable time and damaged assets, as the bank cannot afford the time to make money. As for network risk, unauthorized breaks into file systems through the command line interface, which means they have comprised the network system, taken control, and implemented ransomware. The company might have to encounter legal consequences because it deals with too many losses and damage to its finances and economically disrupts organizations and banks.

**Correlation**

CVE-2024-23897 is a critical vulnerability analyzed and discussed in several tech news and tech articles that affect software applications that permit threat actors or attackers to access arbitrary files and execute malicious commands via CLI (a good environment to execute compromising stuff). Regarding the ransomware attack on the C-edge Technologies company, this CVE vulnerability can be seen as the gateway for further attacks. Take advantage of that; attackers could gain unauthorized access if the company lacks knowledge (or ignored) on this CVE report, crash transaction business with ransomware, bring offline services, and steal multiple valuable payment credentials right after.

Understanding vulnerabilities in real-world events is crucial because it allows organizations to plan and find practical solutions to prevent and replicate a backup version of network and software applications, with assumptions that attackers can threaten them at any moment. Organizations can implement and enhance more defensive layers. With this understanding, they can replicate the fake situation and safely evaluate the VM environment out of those layers within the government permission range or legal tool to use. With this VM test,

they can practice incident response and recovery plans to mitigate the potential risk. Also, understanding real-world vulnerabilities helps employees among organizations stay alert and resilient under pressure with risk assessment and management. They should apply roles and responsibilities to every attribute of working environments.

**Conclusion**

In summary, this CVE-2024-23897 highlights the extreme critical vulnerabilities that remain threats to the digital community and are linked to troublesome incidents, especially the damage to the Tech companies and overall infrastructure nationwide, the theft of sensitive bank-payment data. Such incidents remind organizations and individuals to stay cautious, continuously threat intelligence, and stay informed with CVE. This habit practice allows them to stay ahead in detecting and preventing to minimize the exploitation potential. It is beneficial to know the impact measurements and affected products to maintain regulation, better security awareness, and risk management. Organizations should adopt strict regulation policies from strong companies stay updated on security patches and apply restrictions and guidelines. They should train staff and employees to be resilient under pressure when responding to incidents, mitigate techniques, and, if necessary, upgrade security defense tools. With those approaches, organizations protect their integrity, availability, and confidentiality of secure assets, insider resources, and customers' sensitive data.

**References**

*CVE-2024-23897 Detail*. NVD. (2024a, January 24).

https://nvd.nist.gov/vuln/detail/cve-2024-23897#VulnChangeHistorySection

Franklin, M. (2024). Sourcing and Accessing Threat Intelligence. CSUF.

https://csufullerton.instructure.com/courses/3453673/pages/sourcing-and-accessing-threat-intelligence-2?module\_item\_id=85541790

Greig, J. (2024, August 16). *Ransomware attack on Indian payment system traced back to Jenkins Bug*. Cyber Security News | The Record,

https://therecord.media/jenkins-vulnerability-india-npci-ransomware-attack

*Jenkins Security Advisory. Jenkins security advisory 2024-01-24. (2024, January 24).*

https://www.jenkins.io/security/advisory/2024-01-24/

Nizry, Y. (2024, January 24). Excessive Expansion: Uncovering Critical Security Vulnerabilities in Jenkins. *Sonar*,

https://www.sonarsource.com/blog/excessive-expansion-uncovering-critical-security-vulnerabilities-in-jenkins

Tunggal, A. T. (n.d.). *What is a CVE? common vulnerabilities and exposures explained: Upguard*. Upguard,

https://www.upguard.com/blog/cve