Jenkins Patches High-Severity Vulnerabilities in Multiple Plugins

CVE-2023-40336

What is CVSS?

CVSS stands for the Common Vulnerability Scoring System. It's a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way. The goal of CVSS is to help you compare vulnerabilities in different applications – and from different vendors - in a standardized, repeatable, vendor agnostic approach.

CVSS generates a score from 0 to 10 based on the severity of the vulnerability. A score of 0 means the vulnerability is less significant than the highest vulnerability with a score of 10, if you're only using CVSS. By using CVSS to prioritize vulnerabilities, you can focus on the most critical ones first and reduce the overall risk to your organization

CVSS Base Score	CVSS Severity Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

What is a CVE?

CVE stands for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws.

First launched in 1999, CVE is managed and maintained by the National Cybersecurity FFRDC (Federally Funded Research and Development Center), operated by the **MITRE Corporation**. CVE entries are brief. They don't include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations. Across these different systems, CVE IDs give users a reliable way to recognize unique vulnerabilities and coordinate the development of security tools and solutions. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number.

CVE Identifiers

When vulnerabilities are verified, a CVE Numbering Authority (CNA) assigns a number. A CVE identifier follows the format of — **CVE-{year}-{ID}**. There are currently 114 organizations, across 22 countries that

are certified as CNAs. These organizations include research organizations, and security and IT vendors. CNAs are granted their authority by MITRE, which can also assign CVE numbers directly.

Once a vulnerability is reported, the CNA assigns it a number from the block of unique CVE identifiers it holds. The CNA then reports the vulnerability with the assigned number to MITRE. Frequently, reported vulnerabilities have a waiting period before being made public by MITRE. This allows vendors to develop patches and reduces the chance that flaws are exploited once known.

When a CVE vulnerability is made public, it is listed with its ID, a brief description of the issue, and any references containing additional information or reports. As new references or findings arise, this information is added to the entry.

Alt link: https://www.youtube.com/watch?v=qfpnJyTl1To

Jenkins:

Jenkins is a fork of a project called Hudson, which was trademarked by Oracle. Hudson was eventually donated to the Eclipse Foundation and is no longer under development. Jenkins development is now managed as an open source project under the governance of the CD Foundation, an organization within the Linux Foundation.

In short:

Jenkins is an open source continuous integration/continuous delivery and deployment (CI/CD) automation software DevOps tool written in the Java programming language. It is used to implement CI/CD workflows, called pipelines.

CVE-2023-40336:

A flaw was found in the Jenkins Folders Plugin. Affected versions of this plugin allow attackers to copy folders.

Alt link: https://www.youtube.com/watch?v=IbNCsQjzTnQ

Reference:

https://www.balbix.com/insights/what-is-a-cve/

https://nvd.nist.gov/vuln/detail/CVE-2023-40336#VulnChangeHistorySection

https://www.infoworld.com/article/3239666/what-is-jenkins-the-ci-server-explained.html

https://access.redhat.com/security/cve/cve-2023-40336

https://www.securityweek.com/jenkins-patches-high-severity-vulnerabilities-in-multiple-plugins/

https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/

https://www.openwall.com/lists/oss-security/2023/08/16/3

Question can be asked:

1. What is CVSS?
2. What is CVE?
3. Severity level for any given CVSS score.
4. What is Jenkins?
5. Explain CVE-2023-40336?