January 29, 2024

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Jenkins published security advisories to address vulnerabilities in multiple products. Included was a critical update for the following:

- Jenkins (core) - multiple versions

Technical Details

Jenkins has a built-in command line interface (CLI) to access Jenkins from a script or shell environment. Jenkins uses the args4j library to parse command arguments and options on the Jenkins controller when processing CLI commands. This command parser has a feature that replaces an @ character followed by a file path in an argument with the file's contents (expandAtFiles). This feature is enabled by default and Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable it.
This allows attackers to read arbitrary files on the Jenkins controller file system using the default character encoding of the Jenkins controller process.

- Attackers with Overall/Read permission can read entire files.
- Attackers **without** Overall/Read permission can read the first few lines of files. The number of lines that can be read depends on available CLI commands. As of publication of this advisory, the Jenkins security team has found ways to read the first three lines of files in recent releases of Jenkins without having any plugins installed and has not identified any plugins that would increase this line count.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-23897, CVE-2024-23898, CVE-2024-23899, CVE-2024-23900
- Jenkins Security Advisory 2024-01-24
- Jenkins Security Advisories