ADV2025_120 Jenkins Security Advisory (3rd April 2025)

Jenkins has published a security advisory to address vulnerabilities affecting the following products on April 2, 2025. It is recommended that you take the necessary precautions to ensure your products are always protected.

- Jenkins weekly – version 2.503 and prior
- Jenkins LTS – version 2.492.2 and prior
- AsakusaSatellite Plugin – version 0.1.1 and prior
- Cadence vManager Plugin – version 4.0.0-282.v5096a_c2db_275 and prior
- monitor-remote-job Plugin – version 1.0 and prior
- Simple Queue Plugin – version 1.4.6 and prior
- Stack Hammer Plugin – version 1.0.6 and prior
- Templating Engine Plugin – version 2.5.3 and prior

For more information on these updates, you can follow this URL:

https://www.jenkins.io/security/advisory/2025-04-02/

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Jenkins Security Advisories. (2025, April 2). Retrieved from Jenkins. https://www.jenkins.io/security/advisories/
- Jenkins security advisory. (2025, April 2). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/jenkins-security-advisory-av25-183