Log4J Vulnerabilities - Aruba Resolutions (Updated to 20 Dec 2021)

The information provided below is referred from https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-019.txt, https://sirt.arubanetworks.com/mailman/listinfo/security alerts_sirt.arubanetworks.com, https://www.arubanetworks.com/website/techdocs/sdwan/docs/advisories/media/security_advisory_notice_apache_log4j2_cve_2021_44228.pdf and https://www.arubanetworks.com/support-services/security-bulletins/.

- **CVE Number**

  2021-44228
  2021-45046

- **Discovery Date**

  Not provided

- **Threat Level**

  Critical

- **Response to Log4j**

Since the discovery of these vulnerabilities, Aruba SIRT has been closely monitoring these threats and how they may affect Aruba products. Aruba SIRT consulted with the product teams, and Aruba Threat Labs performed various tests using POC (Proof of Concept) code against products.

Although some Aruba products use the log4j library, none of them use it in a way that makes them vulnerable to CVE-2021-44228 and CVE-2021-45046. The conclusion of the investigation is that the products listed in the “Unaffected Products” tab are not vulnerable to CVE-2021-44228 and CVE-2021-45046.

- **Affected Aruba Product**

All Silver Peak Orchestrator and legacy GMS products.

- **Unaffected Amazon Products**

1. AirWave Management Platform
2. Aruba Analytics and Location Engine
3. Aruba Central / Central On-Premises
4. Aruba ClearPass Policy Manager
5. Aruba Instant / Aruba Instant Access Points
6. Aruba Instant On
7. Aruba Fabric Composer (AFC) and Plexxi Composable Fabric Manager (CFM) Aruba NetEdit
8. Aruba User Experience Insight (UXI)
9. ArubaOS Wi-Fi Controllers and Gateways
10. ArubaOS SD-WAN Gateways
11. ArubaOS-CX Switches
12. ArubaOS-S Switches

13. HP ProCurve Switches
14. Aruba VIA Client

Other Aruba products not listed above are also not known to be affected by the vulnerability.

- **Aruba SIRT Security Procedures**

To receive Security Advisory updates, subscribe to notifications at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com Complete information on reporting security vulnerabilities in Aruba Networks products and obtaining assistance with security incidents is available at:

https://www.arubanetworks.com/support-services/security-bulletins/

For reporting *NEW* Aruba Networks security issues, email can be sent to aruba sirt(at)hpe.com. For sensitive information we encourage the use of PGP encryption. Our public keys can be found at:

https://www.arubanetworks.com/support-services/security-bulletins/