February 29, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that HPE published a security advisory to address vulnerabilities in the following product:

- Aruba ClearPass Policy Manager 6.12.x – version 6.12.0
- Aruba ClearPass Policy Manager 6.11.x – version 6.11.6 and prior
- Aruba ClearPass Policy Manager 6.10.x – version 6.10.8 Hotfix Q4 2023 and prior
- Aruba ClearPass Policy Manager 6.9.x – version 6.9.13 Hotfix Q4 2023 and prior

Exploitation of some of these vulnerabilities could result in remote code execution.

Technical Details
An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. The impact of this vulnerability on ClearPass Policy Manager has not been confirmed, but the version of Apache Struts has been upgraded for mitigation. HPE Aruba Networking is not aware of any malicious exploitation of this vulnerability.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298, CVE-2024-26299, CVE-2024-26300, CVE-2024-26301, CVE-2024-26302, CVE-2023-50164
- HPE Aruba Security Bulletin - ARUBA-PSA-2024-001
- HPE Aruba Security Bulletins