مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Aruba Networking Products

Tracking #:432316308

Date:19-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in HPE Aruba Networking Products that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Multiple vulnerabilities (CVE-2024-42501, CVE-2024-42502, CVE-2024-42503) impacting HPE Aruba Mobility Conductors, Mobility Controllers, and WLAN/SD-WAN Gateways running specific versions of AOS (ArubaOS). These vulnerabilities allow attackers with authenticated access to potentially execute arbitrary code on the underlying operating system.

Vulnerability Details:

- **CVE-2024-42501 (High Severity, CVSSv3 Score: 7.2):** An authenticated path traversal vulnerability exists in AOS. Exploitation could allow an attacker to install unsigned packages and potentially execute arbitrary code or install implants.
- **CVE-2024-42502 (High Severity, CVSSv3 Score: 7.2):** An authenticated remote command execution (RCE) vulnerability exists in the AOS command-line interface (CLI). Exploitation allows an attacker to inject shell commands on the underlying operating system.
- **CVE-2024-42503 (High Severity, CVSSv3 Score: 7.2):** An authenticated RCE vulnerability exists in the Lua package within the AOS CLI. Successful exploitation allows an attacker to run arbitrary commands as a privileged user on the underlying operating system.

Workaround:

Temporary workaround to minimize the risk of exploitation:

- Restrict access to the CLI and web-based management interfaces to a dedicated layer 2 segment/VLAN and/or control access through firewall policies at layer 3 and above.

Affected Versions:

- AOS-10.6.x.x: 10.6.0.2 and below
- AOS-8.12.x.x: 8.12.0.1 and below
- AOS-8.10.x.x: 8.10.0.13 and below

End-of-Maintenance (EOM) Software Versions

The following versions are affected by these vulnerabilities and will not receive patches:

- AOS-10.5.x.x: all
- AOS-10.3.x.x: all
- AOS-8.11.x.x: all
- AOS-8.9.x.x: all
- AOS-8.8.x.x: all
- AOS-8.7.x.x: all
- AOS-8.6.x.x: all
- AOS-6.5.4.x: all
- SD-WAN 8.7.0.0-2.3.0.x: all
- SD-WAN 8.6.0.4-2.2.x.x: all

Fixed Versions:

- AOS-10.7.x.x (version 10.7.0.0 and above)
- AOS-10.6.x.x (version 10.6.0.3 and above)
- AOS-8.12.x.x (version 8.12.0.2 and above)
- AOS-8.10.x.x (version 8.10.0.14 and above)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by HPE Aruba Networking.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04709en_us&docLocale=en_US