BLACKSWAN CYBERSECURITY

THREAT ADVISORY

September 30, 2024

HPE Aruba Access Points Vulnerable to RCE

SUMMARY

Hewlett Packard Enterprise's (HPE) Aruba Networking recently patched three critical vulnerabilities in its Aruba Access Points' Command Line Interface (CLI) for those running AOS-8 and AOS-10, which could allow unauthenticated remote code execution (RCE).

RISK SCORE

CVE-ID	CVSSv3 Score
CVE-2024-42505	9.8
CVE-2024-42506	9.8
CVE-2024-42507	9.8

VULNERABILITY DETAILS

HPE Aruba Networking fixed three critical vulnerabilities in the CLI service of its Aruba Access Points, potentially allowing remote code execution (RCE) by unauthenticated attackers. The vulnerabilities exploit the PAPI UDP port (8211) to gain privileged access and execute arbitrary code on vulnerable devices.

AFFECTED PRODUCTS

- AOS-10.6.x.x: 10.6.0.2 and below
- AOS-10.4.x.x: 10.4.1.3 and below
- Instant AOS-8.12.x.x: 8.12.0.1 and below
- Instant AOS-8.10.x.x: 8.10.0.13 and below

The following software versions that are End of Support Life (EoSL) are affected by these vulnerabilities and were not addressed by HPE:

- AOS-10.5.x.x: all
- AOS-10.3.x.x: all
- Instant AOS-8.11.x.x: all
- Instant AOS-8.9.x.x: all
- Instant AOS-8.8.x.x: all
- Instant AOS-8.7.x.x: all
- Instant AOS-8.6.x.x: all
- Instant AOS-8.5.x.x: all
- Instant AOS-8.4.x.x: all
- Instant AOS-6.5.x.x: all
- Instant AOS-6.4.x.x: all

SOLUTION

- AOS-10.7.x.x: 10.7.0.0 and above
- AOS-10.6.x.x: 10.6.0.3 and above
- AOS-10.4.x.x: 10.4.1.4 and above
- Instant AOS-8.12.x.x: 8.12.0.2 and above
- Instant AOS-8.10.x.x: 8.10.0.14 and above
- Customers running End of Support Life (EoSL) software to upgrade to a supported version as soon as possible.

RECOMMENDATIONS

- Apply the latest security updates for affected Aruba Access Points from the HPE Networking Support Portal.
- All devices running End of Support Life (EoSL) software must upgrade to a supported version as soon as possible.
- For Instant AOS-8.x devices, enable "cluster-security" as a temporary workaround.
- Block access to the PAPI UDP port (8211) from untrusted networks for AOS-10 devices.

REFERENCES

- https://www.bleepingcomputer.com/news/security/hpe-aruba-networking-fixes-three-critical-rce-flaws-impacting-its-access-points/
- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US