May 15, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware HPE published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following products:

- ArubaOS 10.5.x.x – version 10.5.1.0 and prior
- ArubaOS 10.4.x.x – version 10.4.1.0 and prior
- ArubaOS 10.3.x.x – all versions
- InstantOS 8.11.x.x – version 8.11.2.1 and prior
- InstantOS 8.10.x.x – version 8.10.0.10 and prior
- InstantOS 8.9.x.x – all versions
- InstantOS 8.8.x.x – all versions
- InstantOS 8.7.x.x – all versions
- InstantOS 8.6.x.x – version 8.6.0.23 and prior
- InstantOS 8.5.x.x – all versions
- InstantOS 8.4.x.x – all versions
- InstantOS 6.5.x.x – all versions
- InstantOS 6.4.x.x – all versions

Technical Details

There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.

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-2024-31466 CVE-2024-31467 CVE-2024-31468 CVE-2024-31469 CVE-2024-31470 CVE-2024-31471 CVE-2024-31472 CVE-2024-31473 CVE-2024-31474 CVE-2024-31475 CVE-2024-31476 CVE-2024-31477 CVE-2024-31478 CVE-2024-31479 CVE-2024-31480 CVE-2024-31481 CVE-2024-31482 CVE-2024-31483
- HPE Security Bulletin - hpesbnw04647
- HPE Security Bulletin Library