May 1, 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 a security advisory to address vulnerabilities in the following product:

- HPE Aruba Networking ArubaOS – multiple versions

Technical Details

There is a buffer overflow vulnerability in the underlying Utility daemon 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 this vulnerability 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-2024-26305 CVE-2024-26304 CVE-2024-33511 CVE-2024-33512 CVE-2024-33513 CVE-2024-33514 CVE-2024-33515 CVE-2024-33516 CVE-2024-33517 CVE-2024-33518
- HPE Security Bulletin - hpesbst04640en_us
- HPE Security Bulletin Library
-