Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware HPE Aruba Networking has released patches for Aruba access points running InstantOS and ArubaOS 10 that address multiple security vulnerabilities.

Technical Details

- **Unauthenticated Buffer Overflow Vulnerabilities in Services Accessed by the PAPI Protocol**
  There are buffer overflow vulnerabilities in multiple underlying services 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 result in the ability to execute arbitrary code as a privileged user on the underlying operating system. (CVE-2023-35980, CVE-2023-35981, CVE-2023-35982)

- **Information Disclosure in Kernel**
  There is an information disclosure vulnerability in the kernel used by Aruba access points running InstantOS and ArubaOS 10. (CVE-2022-25667)

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

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

References

- CVE-2022-25667, CVE-2023-35980, CVE-2023-35981, CVE-2023-35982
- https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-009.txt