

Overall Rating - High



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

Summary

The Vulnerability and Risk Management (VRM) Team is aware HPE has published security bulletins to address vulnerabilities in the following products:

- Aruba CX Switches – multiple versions and models
- HPE Fibre Channel and SAN Switches with Brocade Fabric OS – multiple versions and models

Technical Details

- **Authenticated Command Injection Vulnerability in AOS-CX Command Line Interface**
An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX.
- **HPE Fibre Channel and SAN Switches with Brocade Fabric OS (FOS), Multiple Vulnerabilities**
Potential security vulnerabilities have been identified in HPE Fabric OS. These vulnerabilities could be remotely or locally exploited to allow multiple vulnerabilities.

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

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- [HPE Security Bulletin - hpesbnw04498en_us](#)
- [HPE Security Bulletin - hpesbst04494en_us](#)
- [HPE Security Bulletins](#)