January 23, 2024

Overall Rating - High

BRITISH COLUMBIA

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

Summary

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

- HPE Superdome Flex Server – versions prior to 90.18
- HPE Superdome Flex 280 Server – versions prior to v1.70.14
- HPE Compute Scale-up Server 3200 – versions prior to v1.10.342
- HPE Unified Mediation Bus – versions prior to 4.4

Exploitation of these vulnerabilities could result in remote exploitation.

Technical Details

Potential security vulnerabilities have been identified in HPE Superdome Flex, Superdome Flex 280 and Compute Scale-up Server 3200 server platforms firmware. These vulnerabilities could be exploited to allow remote code execution, denial of service, information disclosure, DNS cache poisoning and network session hijacking.

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

- CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237
- HPE Security Bulletin - hpesbhf04576en_us
- HPE Security Bulletin – hpesbgn04569en_us
- HPE Security Bulletins