

**Overall Rating: Critical**

This is a technical bulletin intended for technical audiences.

### Summary

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

- HPE Aruba Networking – multiple products and versions
- HPE CrayXD665 – versions prior to BMC 1.14
- HPE CrayXD670 – versions prior to BMC 1.14
- HPE Moonshot1500 2.0 Chassis Manager Module – versions prior to v4.0-b43

### Technical Details

Potential security vulnerabilities have been identified in certain HPE Cray Servers using AMI MegaRac SPX Software. These vulnerabilities could be locally exploited to allow memory corruption, buffer overflow, and untrusted pointer dereference.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at [vulnerabilityandriskmanagement@gov.bc.ca](mailto:vulnerabilityandriskmanagement@gov.bc.ca)

### References

- [CVE-2024-3596 CVE-2023-3043 CVE-2023-34332 CVE-2023-34333 CVE-2023-37293 CVE-2023-37294 CVE-2023-37295 CVE-2023-37296 CVE-2023-37297 CVE-2019-17594 CVE-2019-17595 CVE-2019-9511 CVE-2019-9513 CVE-2020-16156 CVE-2020-19131 CVE-2020-19144 CVE-2021-30560 CVE-2021-32292 CVE-2021-3618 CVE-2021-39537 CVE-2021-41617 CVE-2021-4189 CVE-2021-4209 CVE-2021-46823 CVE-2021-46828 CVE-2022-0391 CVE-2022-0934 CVE-2022-1183 CVE-2022-1354 CVE-2022-1355 CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2022-22576 CVE-2022-22747 CVE-2022-2469 CVE-2022-24903 CVE-2022-2509 CVE-2022-2519 CVE-2022-2520 CVE-2022-2521 CVE-2022-27404 CVE-2022-27405 CVE-2022-27406 CVE-2022-27774 CVE-2022-27775 CVE-2022-27776 CVE-2022-27780 CVE-2022-27781 CVE-2022-27782 CVE-2022-2795 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-2881 CVE-2022-2906 CVE-2022-29155 CVE-2022-2928 CVE-2022-2929 CVE-2022-29458 CVE-2022-2953 CVE-2022-3080 CVE-2022-3094 CVE-2022-31782 CVE-2022-34480 CVE-2022-34526 CVE-2022-3479 CVE-2022-3570 CVE-2022-3597 CVE-2022-3598 CVE-2022-3599 CVE-2022-3627 CVE-2022-3736 CVE-2022-37454 CVE-2022-38177 CVE-2022-38178 CVE-2022-3821 CVE-2022-3924 CVE-2022-3970 CVE-2022-40090 CVE-2022-40674 CVE-2022-40899 CVE-2022-41741 CVE-2022-41742 CVE-2022-42919 CVE-2022-43680 CVE-2022-4415 CVE-2022-45061 CVE-2022-45873 CVE-2022-48281](#)
- [HPE Security Bulletin – HPE Aruba Networking](#)
- [HPE Security Bulletin – HPE Cray Servers](#)
- [HPE Security Bulletin – HPE Moonshot 1500 Chassis Manager 2.0](#)
- [Alert - RADIUS Protocol Susceptible to Forgery Attacks](#)
- [HPE Security Bulletin Library](#)