

## Overall Rating: High



This is a technical bulletin intended for technical audiences.

### Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of HPE ProLiant DL/XL Servers and HPE Cray Supercomputer vulnerabilities. The vulnerability affects HPE ProLiant DL325 Gen10 Plus server - Prior to 2.84 (HFP 23.9), HPE ProLiant DL385 Gen10 Plus server - Prior to 2.84 (HFP 23.9), HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.84 (HFP 23.9), HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.84 (HFP 23.9), HPE Cray EX235a Accelerator Blade - Prior to 1.8.0 (HFP 24.3.1), HPE Cray EX235n Server - Prior to 1.3.1 (HFP 23.9), HPE Cray EX425 Compute Blade - Prior to 1.7.2 (HFP 23.9) - Gen 2, and Gen 3 EPYC Processors, and HPE Cray EX4252 Compute Blade - Prior to 1.4.0 (HFP 23.8).

### Technical Details

Potential security vulnerabilities have been identified in certain HPE ProLiant DL/XL servers and HPE Cray Supercomputer using certain AMD EPYC processors. These vulnerabilities could be locally exploited to allow multiple vulnerabilities, including Arbitrary Code Execution, Code Execution, Denial of Service (DoS), Elevated Privileges, Buffer Overflow.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

### 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-2021-26345, CVE-2021-46766, CVE-2021-46774, CVE-2022-23820, CVE-2022-23830, CVE-2023-20519, CVE-2023-20521, CVE-2023-20526, CVE-2023-20533, CVE 2023-20566
- [HPESBCR04657 rev.1 - Certain HPE ProLiant DL/XL Servers and HPE Cray Supercomputer Using Certain AMD EPYC Processors, Multiple Vulnerabilities](#)
- [VRM Vulnerability Reports](#)