July 4, 2024

**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 a HPE Cray Server vulnerability. The vulnerability affects HPE Cray EX235a Accelerator Blade prior to BIOS 1.8.0 in HFP 24.3.1, HPE Cray EX235n Server prior to BIOS 1.3.1 in HFP 23.9, HPE Cray EX425 Compute Blade prior to BIOS 1.7.2 in HFP 23.9 and HPE Cray EX4252 Compute Blade prior to BIOS 1.4.0 in HFP 23.8.

## Technical Details

A potential security vulnerability has been identified in certain HPE Cray Servers using certain AMD EPYC processors. The vulnerability could be locally exploited to allow arbitrary code execution vulnerability.

| **Exploitability Metrics** |
| --- |
| Attack Vector: Local |
| Attack Complexity: Low |
| Privileges Required: None |
| User Interaction: None |

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 atVulnerabilityandRiskManagement@gov.bc.ca.

## References

- CVE-2023-20577
- HPESBCR04666 rev.1 - Certain HPE Cray Servers Using Certain AMD EPYC Processors, AMD-SB-7009: AMD Processor Security Notice, Local Arbitrary Code Execution Vulnerability
- VRM Vulnerability Reports