June 12, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Lenovo published vulnerabilities. The vulnerability affects versions <> and <>.

Technical Details

Potential weaknesses (CVE-2022-23829) in AMD's SPI protection features may allow an attacker to bypass the native System Management Mode (SMM) ROM protections. Please refer to the AMD SPI Lock Bypass Vulnerability below for additional details and a complete impacted product listing.

Additionally, a privilege escalation vulnerability (CVE-2024-4696) was reported in Lenovo Service Bridge that could allow operating system commands to be executed if a specially crafted link is visited. Upgrade to the Lenovo Service Bridge version 5.0.2.17 or later.

The Lenovo Service Bridge add-in for Lenovo Vantage is not affected by this issue.

Finally, Lenovo announced Multi-vendor BIOS Security Vulnerabilities

- AMI has released security enhancements for AMI BIOS. No CVE available.
- Insyde reported a potential vulnerability that could allow a privileged attacker to modify SMRAM variables. INSYDE-SA-2023067: CVE-2023-47252
- Insyde reported potential SMM memory corruption vulnerabilities that could allow an attacker to escalate privileges. INSYDE-SA-2024001: CVE-2024-25078, CVE-2024-25079, CVE-2024-27353
- Intel reported potential security vulnerabilities in some Intel BIOS Guard and Platform Properties Assessment Module (PPAM) firmware that may allow escalation of privilege. INTEL-SA-00814: CVE-2023-27504, CVE-2023-28402, CVE-2023-28383
- Intel reported a potential security vulnerability in some Intel Processors that may allow information disclosure. INTEL-SA-01051: CVE-2023-45733
- Intel reported a potential security vulnerability in Intel Core Ultra Processors that may allow denial of service. INTEL-SA-01052: CVE-2023-46103
- Intel reported potential security vulnerabilities in some Intel Trust Domain Extensions (TDX) module software that may allow escalation of privilege. INTEL-SA-01036: CVE-2023-45745, CVE-2023-47855
- Phoenix Technologies reported potential buffer overflow vulnerabilities that may allow an attacker with local privileges to execute arbitrary code. CVE-2024-1598, CVE-2024-0762

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-2022-23829, CVE-2024-0084, CVE-2024-0085, CVE-2024-0086, CVE-2024-0089, CVE-2024-0090, CVE-2024-0091, CVE-2024-0092, CVE-2024-0093, CVE-2024-0094, CVE-2024-0099, CVE-2024-4696
- LEN-95137 AMD SPI Lock Bypass Vulnerability

- LEN-163429 Lenovo Service Bridge Vulnerability
- LEN-163020 NVIDIA GPU Display Driver - June 2024
- VRM Vulnerability Reports