May 17, 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 Lenavo security update. Please refer to the numerous Lenovo products impacted by this advisory in the reference links below.

Technical Details

Numerous vulnerabilities impacting Lenovo devices have been reported. Detailed information is available in the reference section of this notification.

- 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 Security Advisory 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 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

The impact of these vulnerabilities may be discovered in the Lenovo vendor notifications in the references below. Additionally, links are provided to detailed information in the NVD CVE's.

Exploitability Metrics
Attack Vector: Network
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

- AMI’s Product Security
- Insyde Security Advisory 2023067
- Insyde Security Advisory 2024001
- INTEL-SA-00814
- INTEL-SA-01052
- INTEL-SA-01036
- Phoenix Technologies
- CVE-2023-27504, CVE-2023-28383, CVE-2023-28402, CVE-2023-45733, CVE-2023-45745, CVE-2023-46103, CVE-2023-47252, CVE-2023-47855, CVE-2024-0762, CVE-2024-1598, CVE-2024-25078, CVE-2024-25079, CVE-2024-27353, CVE-2024-21828
- Multi-vendor BIOS Security Vulnerabilities (May, 2024)
- Intel Ethernet Controller Administrative Tools Installer Software Advisory
- VRM Vulnerability Reports