March 22, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Lenovo vulnerabilities.

Technical Details

Fingerprint Reader Vulnerabilities

An authentication bypass vulnerability was reported in Lenovo devices with Synaptics fingerprint readers that could allow an attacker with physical access to replay fingerprints and bypass Windows Hello authentication (CVE-2024-23592). Additionally, a vulnerability in some fingerprint readers that could allow an attacker with physical access to bypass Windows Hello authentication (CVE-2023-50430). Finally, a vulnerability in some match-on-chip fingerprint readers that could allow an attacker with physical access to bypass Windows Hello authentication (CVE-2024-0454).

Multi-vendor BIOS Security Vulnerabilities (March, 2024)

Multiple issues have been reported in regard to Lenovo BIOS Security Vulnerabilities:

- a SMM callout vulnerability that could allow a privileged attacker to escalate privileges and execute arbitrary code (CVE-2020-5952).
- a buffer overflow vulnerability that may allow an attacker with local privileged access to execute arbitrary code (CVE-2023-39281).
- a vulnerability that could allow an attacker to modify UEFI variables (CVE-2023-28149).
- a SMM memory corruption vulnerability that may allow escalation of privileges (CVE-2023-39283).
- a vulnerability that may allow bypass of security mechanisms (CVE-2023-39284).
- Intel reported potential security vulnerabilities in some 4th Generation Intel® Xeon Processors when using Intel Software Guard Extensions (SGX) or Intel Trust Domain Extensions (TDX) that may allow escalation of privilege or information disclosure (CVE-2023-32666).
- Intel reported a protection mechanism failure in some 3rd and 4th Generation Intel Xeon Processors when using Intel SGX or Intel TDX that may allow a privileged user to potentially enable escalation of privilege via local access (CVE-2023-22655).
- Intel reported a potential security vulnerability in some Intel Atom Processors that may allow information disclosure (CVE-2023-28746).
- Intel reported a potential security vulnerability in BIOS firmware for some Intel Processors that may allow escalation of privilege (CVE-2023-32282).
- Intel reported a potential security vulnerability in the bus lock regulator mechanism for some Intel Processors that may allow denial of service (CVE-2023-39368).
- Intel reported a potential security vulnerability in some Intel Processors that may allow information disclosure (CVE-2023-38575).
- A potential SMM callout vulnerability was reported in some Lenovo Consumer Notebook products that may allow a local attacker with elevated privileges to write stack memory to NVRAM (CVE-2023-5912).

This vulnerability is rated as a **CRITICAL** risk. A software update(s) 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.

References

- CVE-2024-23592, CVE-2023-50430, CVE-2024-0454
- CVE-2020-5952, CVE-2022-30426, CVE-2023-22655, CVE-2023-28149, CVE-2023-28746, CVE-2023-32282, CVE-2023-32666, CVE-2023-38575, CVE-2023-39281, CVE-2023-39283, CVE-2023-39284, CVE-2023-39368, CVE-2023-5912
- Fingerprint Reader Vulnerabilities
- Multi-vendor BIOS Security Vulnerabilities (March, 2024)
- VRM Vulnerability Reports