August 30, 2023

Overall rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of vulnerabilities in three third-party bootloaders that could allow Secure Boot security enforcement to be bypassed by an attacker with physical or administrator access. =

Technical Details

Vulnerabilities in three third-party bootloaders that could allow Secure Boot security enforcement to be bypassed by an attacker with physical or administrator access and allow unauthorized code execution during the boot process. Lenovo client and server products support Secure Boot. All boot loaders – vulnerable or otherwise - are allowed to execute by design when Secure Boot is disabled.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: Low
Privileges Required: High
User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. A software patch 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-2022-34301, CVE-2022-34302, CVE-2022-34303
- Third-party Bootloader Vulnerabilities
- Lenovo Product Security Advisories and Announcements

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca