December 8, 2023

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 Lenovo vulnerabilities. Vulnerabilities were reported in the image parsing libraries in AMI, Insyde and Phoenix BIOS which are used to parse personalized boot logos that are loaded from the EFI System Partition that could allow a local attacker with elevated privileges to trigger a denial of service or arbitrary code execution.

Technical Details

Specifically, improper Input Validation in the processing of user-supplied splash screen during system boot in Phoenix SecureCore Technology 4 potentially allows denial-of-service attacks or arbitrary code execution.

Additionally, AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a BMP Logo file with dangerous type by Local access. A successful exploit of this vulnerability may lead to a loss of Confidentiality, Integrity, and/or Availability. AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a PNG Logo file with dangerous type by Local access. A successful exploit of this vulnerability may lead to a loss of Confidentiality, Integrity, and/or Availability.

Finally, a LogoFAIL issue was discovered in BmpDecoderDxe in Insyde InsydeH2O with kernel 5.2 before 05.28.47, 5.3 before 05.37.47, 5.4 before 05.45.47, 5.5 before 05.53.47, and 5.6 before 05.60.47 for certain Lenovo devices. Image parsing of crafted BMP logo files can copy data to a specific address during the DXE phase of UEFI execution. This occurs because of an integer signedness error involving PixelHeight and PixelWidth during RLE4/RLE8 compression.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Privileges Required: High
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.

References

- CVE-2023-5058, CVE-2023-39538, CVE-2023-39539, CVE-2023-40238
- BIOS Image Parsing Function Vulnerabilities (LogoFAIL)
- VRM Vulnerability Reports