Reducing the Risk of UEFI's Hidden Security Challenges

Memory management vulnerabilities fundamentally impacting more than 280 million computers were discovered in late 2022 due to various implementations of software built using the Unified Extensible Firmware Interface (UEFI) standard. SEI research has informed both industry and government responses to this deeply rooted problem.

UEFI-based software, installed as part of firmware, is crucial for initializing computer hardware at startup and managing the ongoing interaction between hardware and the operating system (OS). UEFI-based software, often invisible to users, is an appealing target for attackers. Those who can exploit UEFI software vulnerabilities can establish persistence and remain invisible to most security software and often even to the OS.

After UEFI-exploiting malware such as BlackLotus was confirmed in early 2023, SEI senior information security architect Vijay Sarvepalli led a study of UEFI software security. Leveraging the SEI's experience in coordinating identified vulnerabilities and establishing secure coding standards, Sarvepalli produced five recommendations for securing the UEFI ecosystem, detailed in a 2023 white paper.

Both the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have cited Sarvepalli's work to enhance their research and improve the UEFI ecosystem. The research has had the largest impacts on improving UEFI memory management vulnerability and UEFI digital signature and revocation maturity.

Exploits like BlackLotus continue to target UEFI software. However, the SEI's work with the diverse stakeholders in UEFI's supply chain has improved UEFI security throughout the vulnerability management lifecycle. The CERT Coordination Center has engaged with vendors and researchers on mitigations across the UEFI ecosystem, such as memory management, digital signature and revocation, privilege separation, supply-chain security, and automated patching.

The SEI's continued research and outreach through supply-chain channels has been in the spirit of Executive Order 14028 on improving the nation's cybersecurity. As a federally funded research and development center, the SEI is in a unique position as a neutral third party to raise public awareness and impartially influence vendors to resolve this problem.

"The promise of this work is to continue to make this type of hidden software more secure," said Sarvepalli. "We can shine light on the security needed not only for UEFI, but other critical, invisible software."

"We can shine light on the security needed not only for UEFI, but other critical, invisible software."

VIJAY SARVEPALLI, Senior Information Security Architect, SEI CERT Division