CIRT.GY Guyana National Computer Incident Response Team

AL2025_33 New Secure Boot Flaw Enables Bootkit Malware Installation (June 17, 2025)

Description

Security researchers have disclosed a critical Secure Boot bypass vulnerability, tracked as CVE-2025-3052, that allows attackers to disable security protections on PCs and servers, enabling the installation of persistent bootkit malware. This flaw affects nearly all systems that trust Microsoft's "UEFI CA 2011" certificate, which includes most modern hardware supporting Unified Extensible Firmware Interface (UEFI) Secure Boot. The vulnerability, discovered by Binarly researchers, exploits a legitimate BIOS update utility signed with Microsoft's certificate, compromising the entire UEFI supply chain and allowing attackers to execute unsigned code during the boot process.

Attack Details

The vulnerability originates from a memory corruption flaw in a BIOS update utility signed with Microsoft's UEFI CA 2011 certificate. This utility reads a user-writable NVRAM variable (IhisiParamBuffer) without proper validation, allowing attackers with administrative access to the operating system to manipulate this variable. By modifying the variable, attackers can write arbitrary data to memory lo- cations during the UEFI boot process, overwriting the gSecurity2 structure; a critical component enforcing Secure Boot checks. Setting the LoadImage function to zero disables Secure Boot, enabling the execution of unsigned UEFI modules, such as bootkits.

Bootkit malware is particularly dangerous as it runs before the operating system loads, evading traditional security software and persisting even after OS reinstallation. The vulnerable module, available online since at least late 2022, affects over 50 device manufacturers relying on Linux boot modules. Binarly's proof-of-concept exploit demonstrated the ability to disable Secure Boot, highlighting the severity of the flaw. Microsoft addressed this issue in the June 2025 Patch Tuesday by blacklisting 14 cryptographic hashes tied to the affected firmware modules in the Secure Boot forbidden database (dbx).

Remediation

To protect systems from this Secure Boot bypass vulnerability, organizations and users should implement the following measures:

- **Apply Security Updates**
  - Install the June 2025 Patch Tuesday updates from Microsoft to blacklist the 14 affected firmware modules in the Secure Boot dbx.
  - Check with device manufacturers for firmware updates addressing CVE-2025-3052.

- **Physical Security**
  - Restrict physical access to devices, as exploitation requires brief access to modify the boot loader (e.g., via IGEL booting).
  - Secure devices in public or shared environments to prevent unauthorized access.
- **Endpoint Protection**
  - Deploy Endpoint Detection and Response (EDR) solutions to monitor for unauthorized boot process modifications or unsigned UEFI module execution.
  - Enable boot integrity monitoring to detect runtime changes to boot services.
- **Access Control**
  - Limit administrative privileges to reduce the risk of attackers gaining the system-level ac- cess required to exploit the flaw.
  - Implement least-privilege policies for all users and applications.
- **Network Monitoring**
  - Monitor for suspicious outbound traffic or unauthorized firmware modifications.
  - Detect anomalies in boot processes, such as disabled NX-bit or unexpected UEFI module execution.
- **Incident Response Readiness**
  - Develop and test an incident response plan to isolate compromised systems and investigate potential bootkit infections.
  - Prepare to reimage systems with verified clean firmware and OS installations.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Binarly. (2025, June 10). Another Crack in the Chain of Trust: Uncovering (Yet Another) Secure Boot Bypass. Retrieved from https://www.binarly.io/blog/another-crack-in-the-chain-of-trust
- Toulas, B. (2025, June 10). New Secure Boot flaw lets attackers install bootkit malware, patch now. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/stealth-falcon-hackers-exploited-windows-webdav-zero-day-to-drop-malware/