CVE-2025-3052: Secure Boot Bypass

Vairav CVE Report

Date: June 11, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A critical new Secure Boot bypass vulnerability, **CVE-2025-3052**, has been identified in Microsoft's UEFI Secure Boot ecosystem. This flaw enables attackers to disable Secure Boot and install persistent bootkit malware. With a high severity CVSS score of **8.2**, successful exploitation can result in security bypasses, persistence mechanisms or full system compromise.

VULNERABILITY DETAILS

CVE-2025-3052

- **Description:** A BIOS-flashing utility, signed with Microsoft's trusted "Microsoft Corporation UEFI CA 2011" certificate, reads a user-controlled NVRAM variable (IhisiParamBuffer) without validation. By modifying this variable (admin/privileged access required), an attacker can write arbitrary data into memory during the UEFI boot process, effectively overwriting the gSecurity2 global variable that enforces Secure Boot. With Secure Boot disabled, any unsigned or malicious UEFI module can be loaded before OS initialization.
- **Impact:** Attackers with administrative privileges can bypass Secure Boot completely, enabling the installation of stealthy bootkits that persist across reboots and OS reinstallation, leading to stealthy system compromise and tampering at the firmware level.
- **CVSS Score:** 8.2 (High)

AFFECTED ENTITIES

- Any system (PC or server) using UEFI Secure Boot and trusting the "Microsoft Corporation UEFI CA 2011" certificate.

EXPLOIT DETAILS

This vulnerability allows local attackers (with administrative privileges) to overwrite Secure Boot enforcement structures early in the boot chain. Using a proof-of-concept, researchers have shown how disabling Secure Boot (via zeroing out gSecurity2) allows the system to load any unsigned UEFI module. An attacker can use this access to install bootkit malware that activates before the OS loads, evading OS-level defenses and surviving reinstallations.

RECOMMENDED ACTIONS

Patch & Upgrade:

- **Install June 2025 Microsoft security updates immediately.** These updates include an updated Secure Boot revocation database (dbx) that contains hashes of the 14 affected modules, including the BIOS-flashing utility.

ADDITIONAL SECURITY MEASURES

- **Immutable Secure Boot policies:** Where supported, lock Secure Boot configuration via firmware password or platform key policy to prevent runtime tampering.
- **Bootkit detection tools:** Deploy UEFI/firmware analysis tools to monitor and alert on any unsigned UEFI modules being executed**.**
- **Periodic Secure Boot validation:** Schedule checks to confirm expected boot variables and health of secure boot keys.
- **Firmware update hygiene:** Only use firmware utilities from vendor-signed, trusted sources and verify signatures against firmware vendor and Microsoft trust chain.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-3052
- https://www.bleepingcomputer.com/news/security/new-secure-boot-flaw-lets-attackers-install-bootkit-malware-patch-now/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com