AVIS DE SECURITE

Objet	Contournement critique de « Secure Boot » via module UEFI signé Microsoft
Niveau de criticité	IMPORTANT
Référence	SNCSIRT-2025-ADS-160
TLP	WHITE

Résumé

Microsoft a corrigé une vulnérabilité critique « CVE-2025-3052 » permettant à un attaquant local d'exploiter un utilitaire BIOS UEFI légitime, signé avec le certificat Microsoft « UEFI CA 2011 », pour désactiver Secure Boot sur des systèmes compatibles UEFI. Le module vulnérable exploite une variable « NVRAM » modifiable (IhisiParamBuffer) sans validation, permettant d'injecter des données arbitraires en mémoire lors du processus de démarrage, avant même le chargement du noyau système.

En modifiant cette variable, un attaquant peut neutraliser la variable critique « gSecurity2 », utilisée par la fonction « LoadImage() » pour appliquer la politique de Secure Boot. Cela rend possible l'exécution de modules UEFI non signés, ouvrant la voie à l'installation de « bootkits » et à la persistance pré-OS, échappant à toute détection par les outils de sécurité classiques.

Microsoft a publié, lors du Patch Tuesday du 10 juin 2025, une mise à jour de la base de révocation Secure Boot (dbx), qui contient les 14 empreintes SHA-256 (hashes) des modules signés identifiés comme vulnérables. Tous les systèmes utilisant Secure Boot doivent appliquer immédiatement cette mise à jour pour bloquer l'exécution de ces modules.

Indicateurs de compromission (IoCs)

- Exemples de hashes UEFI révoqués (SHA-256) :
  - c5e9ab92c42bdb0b4204b4cf72d37691f0036e7546476d87a5402d59f29e550a
  - 6b45b7f78224ae5aa6ea2f62167aa2067c32f51a017621e9c47cf74a6a19d91a
  - 7de3749aeb22bb73ec16c15fdd3c8db1ed57b7b8ff8017e6b64d08cb99380e3c
  - 001dcb1bfa0ae2d23925b95d05f59dce83754d4c5d5404b06604bc61fabc6f22
  - *(et 10 autres inclus dans le dbx Microsoft de juin 2025)*
- Certificat compromis : Microsoft UEFI CA 2011
- Variable UEFI manipulée : IhisiParamBuffer (en écriture depuis OS)
- Variable ciblée dans la mémoire UEFI : gSecurity2 (mise à zéro pour désactiver Secure Boot)

Recommandations

- Référence pour la mise à jour : https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-3052
- Installer la mise à jour automatiquement via Windows Update, ou manuellement via les outils de gestion UEFI pour entreprises.
- Intégrer les indicateurs de compromission (IOCs) ci-dessus au niveau des moyens de détection