

# Faille critique dans le firmware UEFI de plusieurs constructeurs

L'US CERT a révélé, lundi 5 janvier 2014, l'existence d'une faille de sécurité critique de certains systèmes UEFI. La vulnérabilité réside dans le script de démarrage (boot script) chargé par le système (durant la séquence d'EFI S3 Resume Boot Path précisément) et utilisé pour réinitialiser la plateforme. Le boot script a notamment accès à la mémoire et aux opérations de lecture/écriture pour simplifier cette réinitialisation. **Le script intervient notamment en amont de la configuration d'importants mécanismes de sécurité de la plate-forme.**

*« Nous avons découvert que sur certains systèmes le boot script réside dans une partie non protégée de la mémoire qui peut être altérée par un attaquant avec accès à la mémoire physique »*, écrivent Rafal Wojtczuk et Corey Kallenberg de MITRE Corporation, un organisme de R&D pour le compte du gouvernement américain sur [l'alerte](#) du Computer Emergency Response Team. En conséquence, une personne malveillante pourrait **contourner la sécurisation du système (Secure Boot) et installer un firmware arbitraire** malgré la présence du micrologiciel signé, et permettre la lecture et l'écriture dans le système de gestion de la mémoire vive (SMRAM), voire de complètement bloquer l'accès au PC. Il faut néanmoins accéder localement à la machine pour opérer les modifications.

## Les UEFI Intel, AMI et Phoenix affectés

Rappelons que l'UEFI (Unified Extensible Firmware Interface) succède au BIOS chez certains constructeurs de cartes mères

(les membres de l'UEFI Forum essentiellement) et s'inscrit comme un logiciel intermédiaire entre le firmware et le système d'exploitation. **Une position critique dans la chaîne de mise en route du PC** et dont l'intégrité est donc primordiale.

Trois des principaux éditeurs d'UEFI ont vu leur système affecté et l'ont, *a priori*, corrigé : Intel, American Megatrends Incorporated (AMI) et Phoenix Technologies. Un doute subsiste pour Dell. Le bug remonte dans les faits à septembre 2014. L'US CERT invite les fabricants de cartes mères, OEM et autres entreprises à **se rapprocher des acteurs concernés pour corriger ce défaut.**

---

### **Lire également**

[Trois installations PHP sur 4 seraient non sécurisées](#)

[Sécurité : Misfortune Cookies, une faille perdue sur des millions de routeurs](#)

[Les MacBooks d'Apple vulnérables aux périphériques Thunderbolt](#)

**crédit photo © Lisa S. – shutterstock**