Forum: Sécurité

Topic: Intel Microcode Boot Loader

Subject: Intel Microcode Boot Loader

Publié par: Tof81

Contribution le : 13/11/2018 18:36:20

Logiciel pour patcher les cartes mères qui n'ont pas été mises à jour pour se protéger contre les vulnérabilités de sécurité, notamment Spectre, par exemple :

https://www.ngohq.com/intel-microcode-boot-loader.html

Comme le microcode est stocké et chargé automatiquement par le BIOS/UEFI, les fabricants de cartes mères doivent émettre une mise à jour. Cependant, les fabricants ne publient normalement des mises à jour de firmware que pour leurs produits les plus récents. De nombreuses cartes-mères restent encore vulnérables jusqu'à ce jour.

Intel Microcode Boot Loader est une solution de contournement pour le problème du microcode sur les cartes mères Intel. Il met à jour le microcode à chaque démarrage du système. Basé sur Intel BIOS Implementation Test Suite (BITS), les utilisateurs n'ont plus besoin de modifier les ROMs BIOS/UEFI pour rester protégés contre les failles de sécurité, les bogues et les erratas.

Cette solution nécessite une clé USB branchée en permanence avec au moins 25 Mo (ou un périphérique similaire) et un BIOS/UEFI prenant en charge le démarrage à partir de périphériques USB.

Instructions :
1. Formatez une clé USB avec le système de fichiers FAT32.
2. Extrayez l'archive sur la clé USB et exécutez install.exe pour la rendre amorçable.
3. Entrez dans le BIOS/UEFI, attribuez la clé USB comme premier périphérique de démarrage et activez le mode de démarrage existant.
4. Le chargeur de démarrage mettra régulièrement à jour le microcode et chargera l'OS.

Notes :
** Cette version inclut les derniers ucodes pour 392 processeurs Intel produits de 1996 à 2018.*
** Les ucodes sont stockés dans le dossier bootmcudb si vous souhaitez les mettre à jour dans le futur.*
** Si vous obtenez l'avertissement'Ucode not found' pendant l'installation, ou prévoyez de déployer sur un autre PC, recherchez le bon ucode (par CPUID) dans bootmcudb et copiez-le dans bootmcu.*

Non testé car carte mère récente et déjà patchée ...

D'autres softs très spécifiques en racine https://www.ngohq.com :

Linpack Xtreme Bootable Media

Linpack Xtreme

Unofficial Spectre Patched BIOS for X58 Motherboards

Firehawk WebSuite

Driver Signature Enforcement Overrider

NGO ATI Optimized Driver

NGO NVIDIA Optimized Driver