RMPrepUSB, Easy2Boot en opstarten via USB

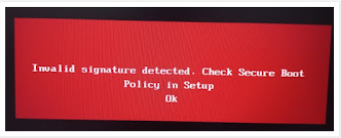
Steve's blog over **RMPrepUSB, Easy2Boot en USB-opstarten** en soms ook andere dingen!
Bezoek **www.rmprepusb.com** voor meer dan 140 Tutorials over USB-opstarten van **www.easy2boot.xyz** voor een unieke USB-multiboot-oplossing.

Vergeet niet te abonneren!

dinsdag 16 augustus 2022

Microsoft heeft Secure Boot multiboot zojuist moeilijker gemaakt!

Nadat de recente Windows-update KB5012 (9 augustus 2022) is uitgebracht, lijkt het erop dat Ventoy op systemen niet meer kan opstarten als Veilig starten. Deze Windows-update kan ook van invloed zijn op het Kaspersky EFI-opstartbestand dat door agFM in E2B wordt gebruikt.



Overzicht

Deze beveiligingsupdate aangebrachte DBX aan in Secure Boot voor de ondersteunde Windows-versies worden vermeld in het gedeelte 'Van toepassing op'. Belangrijke wijzigingen zijn meer:

Windows-apparaten met op Unified Extensible Firmware Interface (UEFI) gebaseerde firmware kunnen draaien met Secure Boot onder. De Secure Boot Forbidden Signature Database (DBX) verwerkt dat UEFI-modules worden geladen. Deze update van modules toe aan de DBX.

Er bestaat een beveiligingsprobleem bij het beveiligen van de beveiligingsfunctie bij opstarten. Eenvaller die het beveiligingslek weet te misbruiken, kan veilig opstarten en niet-vertrouwde software laden.

Deze beveiligingsupdate lost het beveiligingslek op de handtekeningen van de kwetsbare door UEFI-modules aan de DBX toe te voegen.

KB5012170

Zie ook dit bericht.

Invoering

Ventoy (en de 'officiële Ventoy' .img-bestanden die door agFM worden gebruikt) gebruiken een .EFI- bestand met u elk bestand van elke sleutel aan de 'witte lijst' van de BIOS DB kunt toevoegen door MokManager te gebruiken. Dit kan u in elk niet-ondertekenen .efi-zeerbestandd beveiligen en is daarom een duidelijk beveiligingsrisico.

agFM gebruikt een ondertekend Kaspersky EFI-opstartbestand dat een beveiligingsfout bevat, omdat u niet-ondertekende grub2-modules kunt laden. De niet-ondertekende grub2-module kan vervolgens de veilige opstartcontroles uitschakelen en u vervolgens om niet-ondertekende .efi-botbestanden te laden.

Microsoft heeft verschillende Windows-updates uitgebracht die (als je UEFI hebt opgestart naar Windows) zwarte lijstvermeldingen zullen toevoegen aan het niet-vluchtige DBx-RAM van je BIOS, zodat het nu weigert om Secure Boot te beveiligen vanaf de ondeugende EFI's die Microsoft nooit had moeten ondertekenen op de eerste plaats!

Dit laat ons dus met een probleem (dat al enkele jaren aan de gang is) - hoe laden we een multiboot loader/manager zoals Ventoy of agFM (die unsigned grub2) gebruiken. Microsoft zal geen generieke grub2-versie ondertekenen omdat ze je toestaan om andere modules te laden of dd uit te voeren, enz. en dus mogelijk het veilige opstartmechanisme te hacken.

Oplossingen

Ventoy

Voor Ventoy moeten we **Secure Boot uitschakelen** of naar het UEFI BIOS van het doelsysteem gaan en **de DBx-database wissen (verwijderen)** om de zwarte lijstsleutels te verwijderen die door de Windows Update zijn toegevoegd.

Het uitschakelen van Secure Boot in het BIOS is slechts tijdelijk en kan geen kwaad - zolang u eraan denkt om het daarna weer in te schakelen. Maar wat als u het BIOS-wachtwoord niet weet?

een partitie te hebben, omdat ze vaak dezelfde mappen en bestanden gebruiken en de tweede de bestanden van de eerste.

Als u NTFS voor Partitie 1 van de Ventoy USB-drive hebt gebruikt, kunt u de door Rufus ondertekende UEFI_NTFS-opstartbestanden op een FAT Partition 3 op uw drive plaatsen en vervolgens de uitgepakte platte bestanden van uw payload/ISO op Partitie 1 plaatsen. Nogmaals, dit is niet echt een multiboot-oplossing.

Rufus heeft ondertekende NTFS-documenten en een ondertekende .EFI-loader die een ondertekend \EFI\BOOT\BOOTX64.efi-bestand van partitie 1 laadt.

Aanbevolen bericht

Easy2Boot v2.13 is nu vrijgegeven

De door Webnode gehoste site