Nexans switches and UEFI SecureBoot vulnerability - BootHole

KD1752E0

Vulnerability background

Developers in Debian and elsewhere in the Linux community have recently become aware of a severe problem in the GRUB2 bootloader that allows a bad actor to completely circumvent UEFI Secure Boot.

UEFI Secure Boot (SB) is a verification mechanism for ensuring that code launched by a computer's UEFI firmware is trusted. It is designed to protect a system against malicious code being loaded and executed early in the boot process, before the operating system has been loaded.

Unfortunately, a serious bug has been found in the GRUB2 bootloader code which reads and parses its configuration (grub.cfg). This bug breaks the chain of trust; by exploiting this bug, it is possible to break out of the secured environment and load non-signed programs during early boot. This vulnerability was discovered by researchers at Eclypsium and given the name BootHole.

For more information see BSI document CSW-Nr. 2020-226808-10k3. More details are found at https://www.debian.org/security/2020-GRUB-UEFI-SecureBoot/ and https://www.debian.org/security/2020/dsa-4735.

Nexans switches unaffected

Nexans is NOT exposed to the UEFI SecureBoot vulnerability - BootHole.

All types of Nexans Switches are unaffected because Nexans doesn’t use the GRUB2 bootloader and UEFI Secure Boot.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 31.07.2020, Mönchengladbach Germany