PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

30 January 2018
300391657 / pbsa56

Security Advisory for mGuard products [CVE-2018-5441]

Synopsis

The integrity of the mGuard firmware atomic update process cannot be guaranteed under all circumstances

Issue

The mGuard atomic update mechanism relies on internal checksums for the integrity verification of some portions of the update packages. The verification of these internal checksums may not always be performed correctly.

Affected products

The following devices, their derivatives and corresponding Innominate devices are affected:
FL MGUARD RS2000 and FL MGUARD RS4000
TC MGUARD RS2000 3G VPN and TC MGUARD RS4000 3G VPN
FL MGUARD PCI4000 and FL MGUARD PCIE4000
FL MGUARD SMART2 and FL MGUARD CORE TX
FL MGUARD DELTA TX/TX
TC MGUARD RS2000 4G VPN and TC MGUARD RS4000 4G VPN
FL MGUARD GT GT
FL MGUARD CENTERPORT

...

Details

The mGuard only allows the installation of firmware updates digitally signed by Phoenix Contact (Innominate). The atomic update mechanism that was introduced with mGuard 7.2.0 to support the current generation of devices relies on internal checksums for the verification of the internal integrity of some portions of the update packages. As the verification may not always be performed correctly, an attacker might modify firmware update packages.

This vulnerability is present in all mGuard releases since 7.2.0 on the listed devices but does not affect the current mGuard 8.6.1 release.
Firmware images used to completely flash the device are not affected by this vulnerability.

Mitigation

We strongly advise all mGuard users to upgrade to the firmware version 8.6.1.