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

17 December 2020
300498111/pbsa56

Security Advisory for mGuard products

Advisory Title

LAN ports get functional after reboot even if they are disabled in the device configuration

Advisory ID

CVE-2020-12523
VDE-2020-046

Vulnerability Description

For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource (CWE-909).

Affected products

Article no	Article	Affected versions	Fixed version
1010461	TC MGUARD RS4000 4G VZW VPN	< 8.8.3	Download
1010463	TC MGUARD RS4000 4G ATT VPN	< 8.8.3	Download
2701876	FL MGUARD RS4004 TX/DTX	< 8.8.3	Download
2701877	FL MGUARD RS4004 TX/DTX VPN	< 8.8.3	Download
2903440	TC MGUARD RS4000 3G VPN	< 8.8.3	Download
2903586	TC MGUARD RS4000 4G VPN	< 8.8.3	Download
	Innominate mGuard rs4000 4TX/TX	< 8.8.3	Download
	Innominate mGuard rs4000 4TX/TX VPN	< 8.8.3	Download
	Innominate mGuard rs4000 4TX/3G/TX VPN	< 8.8.3	Download

...

Impact

After a reboot, affected mGuard devices may unexpectedly receive or send data on disabled switch ports. This includes the unexpected provision of administrative interfaces. Attackers may try to access confidential data or compromise the availability of mGuard services by flooding or resource exhaustion.

Classification of Vulnerability

Base Score: 5.4
Vector: CVSSv3 AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:L

Temporary Fix / Mitigation

Instead of deactivating by configuration, network cables should be detached from affected switch ports.

Remediation

PHOENIX CONTACT recommends all mGuard users to upgrade to the firmware version 8.8.3.

Acknowledgement

This vulnerability was discovered by SMST Designers & Constructors B.V.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.