Phoenix Contact: Multiple Vulnerabilities in mGuard devices

VDE-2024-039

Last update	08/27/2025 12:00
Published at	09/10/2024 12:00
Vendor(s)	Phoenix Contact GmbH & Co. KG
External ID	VDE-2024-039
CSAF Document	Download ↗

Summary

Confidential data in HTTP query string of user requests.
Incomplete sanitation of user input in administrative web interface.

Impact

Attackers can gain knowledge of confidential user data.
Attackers can escalate their privileges on the system.
Attackers can trigger covert misbehavior within several services.

Affected Product(s)

Model no.	Product name	Affected versions
1357828	FL MGUARD 2102	Firmware <10.4.1
1357850	FL MGUARD 2105	Firmware <10.4.1
1441187	FL MGUARD 4102 PCI	Firmware <10.4.1
1357842	FL MGUARD 4102 PCIE	Firmware <10.4.1
1357840	FL MGUARD 4302	Firmware <10.4.1
1357875	FL MGUARD 4305	Firmware <10.4.1
2702547	FL MGUARD CENTERPORT	Firmware <8.9.3
2702820	FL MGUARD CENTERPORT VPN-1000	Firmware <8.9.3
2702884	FL MGUARD CORE TX	Firmware <8.9.3
2702831	FL MGUARD CORE TX VPN	Firmware <8.9.3
2700967	FL MGUARD DELTA TX/TX	Firmware <8.9.3
2700968	FL MGUARD DELTA TX/TX VPN	Firmware <8.9.3
2700197	FL MGUARD GT/GT	Firmware <8.9.3
2700198	FL MGUARD GT/GT VPN	Firmware <8.9.3
2701274	FL MGUARD PCI4000	Firmware <8.9.3
2701275	FL MGUARD PCI4000 VPN	Firmware <8.9.3
2701277	FL MGUARD PCIE4000	Firmware <8.9.3
2701278	FL MGUARD PCIE4000 VPN	Firmware <8.9.3

Model no.	Product name	Affected versions
2700642	FL MGUARD RS2000 TX/TX VPN	Firmware <8.9.3
2702139	FL MGUARD RS2000 TX/TX-B	Firmware <8.9.3
2701875	FL MGUARD RS2005 TX VPN	Firmware <8.9.3
2700634	FL MGUARD RS4000 TX/TX	Firmware <8.9.3
2200515	FL MGUARD RS4000 TX/TX VPN	Firmware <8.9.3
2702470	FL MGUARD RS4000 TX/TX-M	Firmware <8.9.3
2702259	FL MGUARD RS4000 TX/TX-P	Firmware <8.9.3
2701876	FL MGUARD RS4004 TX/DTX	Firmware <8.9.3
2701877	FL MGUARD RS4004 TX/DTX VPN	Firmware <8.9.3
2700640	FL MGUARD SMART2	Firmware <8.9.3
2700639	FL MGUARD SMART2 VPN	Firmware <8.9.3
2903441	TC MGUARD RS2000 3G VPN	Firmware <8.9.3
1010464	TC MGUARD RS2000 4G ATT VPN	Firmware <8.9.3
2903588	TC MGUARD RS2000 4G VPN	Firmware <8.9.3
1010462	TC MGUARD RS2000 4G VZW VPN	Firmware <8.9.3
2903440	TC MGUARD RS4000 3G VPN	Firmware <8.9.3
1010463	TC MGUARD RS4000 4G ATT VPN	Firmware <8.9.3
2903586	TC MGUARD RS4000 4G VPN	Firmware <8.9.3
1010461	TC MGUARD RS4000 4G VZW VPN	Firmware <8.9.3

Vulnerabilities

Expand / Collapse all

CVE-2024-43388	8.8
CVE-2024-43387	8.8
CVE-2024-43386	8.8
CVE-2024-43385	8.8
CVE-2024-7699	8.8
CVE-2024-43384	8
CVE-2024-43393	6.5
CVE-2024-43392	6.5
CVE-2024-43391	6.5
CVE-2024-43390	6.5
CVE-2024-43389	6.5
CVE-2024-7698	5.7

Mitigation

Access to the administrative interfaces should be granted only to trustworthy users.

Remediation

Phoenix Contact strongly recommends upgrading affected mGuard devices to firmware version 8.9.3 / 10.4.1 or higher which fixes these vulnerabilities.

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination (see https://certvde.com ↗)
- Andrea Palanca from Nozomi Networks Security Research Team for These vulnerabilities were discovered by the Nozomi Networks Security Research Team. We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder. (see https://www.nozominetworks.com/labs ↗)

Revision History

Version	Date	Summary
1.0.0	09/10/2024 12:00	Initial revision.
1.0.1	11/06/2024 12:27	Fix: correct certvde domain, added self-reference
1.0.2	04/10/2025 15:00	Fixed csaf reference URL
1.1.2	08/27/2025 12:00	Update: CWE from CVE-2024-43388, CVE-2024-43389, CVE-2024-43390, CVE-2024-43391, CVE-2024-43392, CVE-2024-43393, CVE-2024-7698, Revision History

Data protection notice

Privacy statement

Share this page

Member of