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

100 years of passion for technology and innovation

13 June 2023
2023/00005

Security Advisory for the FL MGUARD family of devices

Publication Date: 2023-06-13
Last Update: 2023-06-13
Current Version: V1.0

Advisory Title

The FL MGUARD family of devices is affected by two vulnerabilities.

CVE-2022-4304: Timing oracle in RSA decryption
CVE-2023-2673: MAC filtering is not applied to all forwarded packets

Advisory ID

CVE-2022-4304
CVE-2023-2673
VDE-2023-010

Vulnerability Description

CVE-2022-4304: The OpenSSL library contains a bug that leads to a timing oracle when RSA based ciphers are used without forward secrecy for network communication. By sending a very large number of trial messages, an attacker can try to achieve a decryption of encrypted network packets. This affects TLS connections to and from the FL MGUARD as well as VPN

...

connections. The highest risk arises from deferred attempts to decrypt pre-recorded network sessions. The throttling feature of the FL MGUARD can impede but not prevent the attack.

CVE-2023-2673: If a FL MGUARD or TC MGUARD device is operated in static or autodetect stealth mode, UDP packets which are directed to the protected device do not pass the configured MAC filter rules. The issue does not compromise the incoming IPv4 packet filter, which blocks all incoming traffic by default. The issue does not affect multi stealth mode.

Affected products

Article no	Article	Affected versions	Fixed Version
2700642	FL MGUARD RS2000 TX/TX VPN	<= 8.9.0	Download
2701875	FL MGUARD RS2005 TX VPN	<= 8.9.0	Download
2903441	TC MGUARD RS2000 3G VPN	<= 8.9.0	Download
2700634	FL MGUARD RS4000 TX/TX VPN	<= 8.9.0	Download
2200515	FL MGUARD RS4000 TX/TX VPN	<= 8.9.0	Download
2701876	FL MGUARD RS4004 TX/DTX	<= 8.9.0	Download
2701877	FL MGUARD RS4004 TX/DTX VPN	<= 8.9.0	Download
2903440	TC MGUARD RS4000 3G VPN	<= 8.9.0	Download
2702139	FL MGUARD RS2000 TX/TX-B	<= 8.9.0	Download
2702259	FL MGUARD RS4000 TX/TX-P	<= 8.9.0	Download
2702470	FL MGUARD RS4000 TX/TX-M	<= 8.9.0	Download
2701274	FL MGUARD PCI4000	<= 8.9.0	Download
2701275	FL MGUARD PCI4000 VPN	<= 8.9.0	Download
2701277	FL MGUARD PCIE4000	<= 8.9.0	Download
2701278	FL MGUARD PCIE4000 VPN	<= 8.9.0	Download
2700967	FL MGUARD DELTA TX/TX	<= 8.9.0	Download
2700968	FL MGUARD DELTA TX/TX VPN	<= 8.9.0	Download
2700640	FL MGUARD SMART2	<= 8.9.0	Download
2700639	FL MGUARD SMART2 VPN	<= 8.9.0	Download
2702884	FL MGUARD CORE TX	<= 8.9.0	Download
2702831	FL MGUARD CORE TX VPN	<= 8.9.0	Download
2903588	TC MGUARD RS2000 4G VPN	<= 8.9.0	Download
2903586	TC MGUARD RS4000 4G VPN	<= 8.9.0	Download
1010461	TC MGUARD RS4000 4G VZW VPN	<= 8.9.0	Download
1010462	TC MGUARD RS2000 4G VZW VPN	<= 8.9.0	Download
1010463	TC MGUARD RS4000 4G ATT VPN	<= 8.9.0	Download
1010464	TC MGUARD RS2000 4G ATT VPN	<= 8.9.0	Download
2700197	FL MGUARD GT/GT	<= 8.9.0	Download

...

2700198	FL MGUARD GT/GT VPN	<= 8.9.0	Download
2702547	FL MGUARD CENTERPORT	<= 8.9.0	Download
2702820	FL MGUARD CENTERPORT VPN-1000	<= 8.9.0	Download
1357872	FL MGUARD 2102	<= 10.1.1	Download
1357840	FL MGUARD 4302	<= 10.1.1	Download
1357842	FL MGUARD 4102 PCIE	<= 10.1.1	Download
1441187	FL MGUARD 4102 PCI	<= 10.1.1	Download

Impact

CVE-2022-4304: There is a risk that attackers could decrypt network traffic encrypted by the FL MGUARD device.

CVE-2023-2673: There is a risk that attackers could send UDP packets to the protected device which should have been filtered out.

Classification of Vulnerability

CVE-2022-4304
Base Score: 5.9
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: NVD-CWE-OTHER

CVE-2023-2673
Base Score: 5.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L
CWE: CWE-20

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

Temporary Fix / Mitigation

CVE-2022-4304: Do not use RSA based ciphers for encryption of network traffic, use cipher suites with forward secrecy for TLS or IPsec communication and renew vulnerable certificates frequently.

CVE-2023-2673: Configure the incoming IPv4 packet filter carefully to protect clients from potentially malicious UDP packets.

Remediation

The vulnerabilities are fixed in firmware versions 8.9.1 and 10.2.0. We strongly recommend all affected FL MGUARD users to upgrade to this or a later version.

Acknowledgement

CVE-2022-4304: This vulnerability was discovered by Hubert Kario and Dmitry Belyavsky (Red Hat). We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

CVE-2023-2673: This vulnerability was discovered internally.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2023-06-13): Initial publication