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

14 June 2022
300546915

Security Advisory for FL MGUARD, TC MGUARD, mGuard Device Manager and FL WLAN devices

Publication Date: 2022-04-12
Last Update: 2022-06-14
Current Version: V1.1

Advisory Title

A critical vulnerability has been discovered in the OpenSSL library, which is utilized in Phoenix Contact FL MGUARD, TC MGUARD devices, mGuard Device Manager and FL WLAN devices.

Advisory ID

CVE-2022-0778
VDE-2022-013

Vulnerability Description

FL MGUARD and TC MGUARD devices are affected by a possible infinite loop within an OpenSSL library method for parsing elliptic curve parameters. This method is used on parsing cryptographic certificates that contain elliptic curve public keys in compressed form, which may occur on:

- Parsing client certificates for HTTPS administrative login
- Parsing client certificates for SSH administrative login
- Parsing peer certificates for IPsec VPN connections
- Parsing certificates of external servers, including:
  - OpenVPN server
  - Configuration pull server

- Update server

Attackers could try to exploit the vulnerability from remote.
For the mGuard Device Manager only the mdm Installer for Windows is affected.

On FL MGUARD 1102 and FL MGUARD 1105 with mGuardNT 1.5.2 and older, the device can be affected through an adapted certificate. This can occur on connection with a remote logging server, configured for certificate authentication, or an remote authentication server at certificate based authentication.

Affected products

Article no	Article	Affected versions	Fixed version
2700642	FL MGUARD RS2000 TX/TX VPN	<= 8.8.5	Download
2701875	FL MGUARD RS2005 TX VPN	<= 8.8.5	Download
2903441	TC MGUARD RS2000 3G VPN	<= 8.8.5	Download
2700634	FL MGUARD RS4000 TX/TX	<= 8.8.5	Download
2200515	FL MGUARD RS4000 TX/TX VPN	<= 8.8.5	Download
2701876	FL MGUARD RS4004 TX/DTX	<= 8.8.5	Download
2701877	FL MGUARD RS4004 TX/DTX VPN	<= 8.8.5	Download
2903440	TC MGUARD RS4000 3G VPN	<= 8.8.5	Download
2702139	FL MGUARD RS2000 TX/TX-B	<= 8.8.5	Download
2702259	FL MGUARD RS4000 TX/TX-P	<= 8.8.5	Download
2702470	FL MGUARD RS4000 TX/TX-M	<= 8.8.5	Download
2701274	FL MGUARD PCI4000	<= 8.8.5	Download
2701275	FL MGUARD PCI4000 VPN	<= 8.8.5	Download
2701277	FL MGUARD PCIE4000	<= 8.8.5	Download
2701278	FL MGUARD PCIE4000 VPN	<= 8.8.5	Download
2700967	FL MGUARD DELTA TX/TX	<= 8.8.5	Download
2700968	FL MGUARD DELTA TX/TX VPN	<= 8.8.5	Download
2700640	FL MGUARD SMART2	<= 8.8.5	Download
2700639	FL MGUARD SMART2 VPN	<= 8.8.5	Download
2702884	FL MGUARD CORE TX	<= 8.8.5	Download
2702831	FL MGUARD CORE TX VPN	<= 8.8.5	Download
1053405	FL MGUARD SMART2 VPN/K1	<= 8.8.5	Download
1053403	FL MGUARD RS4000 TX/TX VPN/K1	<= 8.8.5	Download
1073940	FL MGUARD PCIE4000 VPN/K2	<= 8.8.5	Download
1073943	FL MGUARD RS4000 VPN/K2	<= 8.8.5	Download
1073944	FL MGUARD PCI4000 VPN/K2	<= 8.8.5	Download
2903588	TC MGUARD RS2000 4G VPN	<= 8.8.5	Download
2903586	TC MGUARD RS4000 4G VPN	<= 8.8.5	Download
1010461	TC MGUARD RS4000 4G VZW VPN	<= 8.8.5	Download
1010462	TC MGUARD RS2000 4G VZW VPN	<= 8.8.5	Download
1010463	TC MGUARD RS4000 4G ATT VPN	<= 8.8.5	Download
1010464	TC MGUARD RS2000 4G ATT VPN	<= 8.8.5	Download

...

2700197	FL MGUARD GT/GT	<= 8.8.5	Download
2700198	FL MGUARD GT/GT VPN	<= 8.8.5	Download
2702547	FL MGUARD CENTERPORT	<= 8.8.5	Download
2702820	FL MGUARD CENTERPORT VPN-1000	<= 8.8.5	Download
2981974	FL MGUARD DM UNLIMITED	<= 1.13.0.1	Download
2702899	FL WLAN 1010	<= 2.70	
2702900	FL WLAN 1011	<= 2.70	
2702534	FL WLAN 1100	<= 2.70	
2702538	FL WLAN 1101	<= 2.70	
1119246	FL WLAN 2010	<= 2.70	
1119248	FL WLAN 2011	<= 2.70	
2702535	FL WLAN 2100	<= 2.70	
2702540	FL WLAN 2101	<= 2.70	
2700718	FL WLAN 5100	<= 3.21	
2701093	FL WLAN 5101	<= 3.21	
2701850	FL WLAN 5102	<= 3.21	
1043193	FL WLAN 5110	<= 3.21	
1043201	FL WLAN 5111	<= 3.21	
1153079	FL MGUARD 1102	<= 1.5.2	Download
1153078	FL MGUARD 1105	<= 1.5.2	Download

Impact

By sending a crafted certificate, attackers may trigger an infinite loop in the receiving service. This may cause the service to become unavailable. Additionally, the availability of other services may be reduced due to high CPU load.

Classification of Vulnerability

CVE-2022-0778
CVSSv3.1 Base Score: 7.5
CVSSv3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE-835

FL MGUARD and TC MGUARD may be vulnerable in the following setups:

- Activated HTTPS administrative access with certificate-based authentication
- Activated SSH administrative access with certificate-based authentication
- Use of IPsec VPN connections with certificate-based authentication
- Use of connections to external servers with certificate-based authentication, including:
  - OpenVPN server
  - Configuration pull server
  - Update server

...

FL WLAN may be vulnerable in the following setup:

- WLAN Client modes with activated certificate-based RADIUS server authentication

The services can be vulnerable, even when they are not configured to use elliptic curve cryptography explicitly.

Temporary Fix / Mitigation

To reduce the possibility of an attack, affected functionality could be deactivated or used only in a way that it is not exposed on untrusted interfaces.

Remediation

This vulnerability is fixed in firmware version 8.8.6. We strongly recommend all affected FL MGUARD and TC MGUARD users to upgrade to this or a later version. FL MGUARD 1102 and FL MGUARD 1105 should be upgraded to version 1.6.0 or higher, which fixes this vulnerability.

PHOENIX CONTACT strongly recommends upgrading FL MGUARD DM UNLIMITED to version 1.13.0.2 or higher, which fixes this vulnerability.

For FL WLAN devices the vulnerability will be fixed in the next regular release. A release date is not yet defined.

Acknowledgement

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

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

History

V1.0 (2022-04-12): Initial publication
V1.1 (2022-06-14): FL MGUARD 1102 and 1105 added