

11 June 2024
2024/00004

Security Advisory for FL MGUARD 1102/1105

Publication Date: 2024-06-11
Last Update: 2024-06-11
Current Version: V1.0

Advisory Title

Unbounded growth of OpenSSL session cache

Advisory ID

[CVE-2024-2511](#)
[VDE-2024-029](#)

Vulnerability Description

The OpenSSL library used in the affected products is vulnerable to an unbounded growth of the session cache in the TLSv1.3 implementation.

Affected products

Article no	Article	Affected versions
1153079	FL MGUARD 1102	< 1.8.0
1153078	FL MGUARD 1105	< 1.8.0

Registered office: Blomberg
Distr. court Lemgo HRA 3746
Personally liable partner:
Phoenix Contact Verwaltungs-GmbH
Management office Blomberg
Distr. court Lemgo HRB 10904
Statutory seat Vaduz/Liechtenstein
Comm. reg. FL-0002.700.066-3

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Pospel-Dölken, Axel Wachholz
Chairman of the Advisory Board:
Dr. Dipl.-Ing. Eberhard Veit

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDE33XXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADE33XXX
IBAN:
DE31 4764 0051 0226 0396 00

Impact

A remote attacker can exhaust all memory by establishing a large number of TLSv1.3 connections to the web interface, causing the device to reboot.

Classification of Vulnerability

[CVE-2024-2511](#)

Base Score: 7.5

Vector: CVSS:3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE: CWE-770 (Allocation of Resources Without Limits or Throttling)

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

Phoenix Contact recommends that customers restrict network access to the device's web interface to as few networks as possible.

Remediation

Phoenix Contact recommends upgrading the firmware of affected devices to version 1.8.0 or higher, which fixes the vulnerability.

Acknowledgement

Phoenix Contact thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2024-06-11): Initial publication