VDE-2025-109: Phoenix Contact: Unbounded growth of the session cache in TCP encapsulation service in FL MGUARD 2xxx and 4xxx firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Feb 10 09:00:00 CET 2026	Engine: 2.5.41
Current release date: Tue Feb 10 09:00:00 CET 2026	Build Date: Thu Jan 08 11:34:25 CET 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 5.9	Severity: Medium
Original language:	Language: en-US
Also referred to: VDE-2025-109, PCSA-2025-00024	

Summary

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

General Recommendation

For general information and recommendations on security measures refer to the mGuard documentation: https://help.mguard.com/en/documentation.

Impact

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

Mitigation

It is recommended to disable TCP encapsulation on affected mGuard devices and use Pathfinder instead.

Remediation

Phoenix Contact strongly recommends upgrading affected mGuard devices to firmware version 10.6.0 or higher which fixes this vulnerability.

Product Description

mGuards are industrial routers and security appliances

Product groups

Affected Products.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

- Firmware 10.5.0 installed on FL MGUARD 2102
- Firmware 10.5.0 installed on FL MGUARD 2105
- Firmware 10.5.0 installed on FL MGUARD 4302
- Firmware 10.5.0 installed on FL MGUARD 4305
- Firmware 10.5.0 installed on FL MGUARD 4102 PCIE
- Firmware 10.5.0 installed on FL MGUARD 4102 PCI
- OpenSSL 3.0.0
- OpenSSL 3.0.13

Fixed Products.

- Firmware 10.6.0 installed on FL MGUARD 2102
- Firmware 10.6.0 installed on FL MGUARD 2105
- Firmware 10.6.0 installed on FL MGUARD 4302
- Firmware 10.6.0 installed on FL MGUARD 4305
- Firmware 10.6.0 installed on FL MGUARD 4102 PCIE
- Firmware 10.6.0 installed on FL MGUARD 4102 PCI
- OpenSSL 3.0.14

Vulnerabilities

Unbounded memory growth with session handling in TLSv1.3 (CVE-2024-2511)

CVE Details

This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation.

This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients.

CVE Impact

An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service

CVE Characterisation

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

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

In the device context, there are two deviations from the original CVSS assessment. An attack - although complex to achieve - can generally be automated, which leads to a rating of low Attack Complexity (AC:L). A successful attack has a temporary effect on the availability of the device, as an automatic reboot occurs when the RAM is fully utilized (A:L).

CVE Description

Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

CWE:	CWE-1325: Improperly Controlled Sequential Memory Allocation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware 10.5.0 installed on FL MGUARD 2102 Order number: 1357828	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware 10.5.0 installed on FL MGUARD 2105 Order number: 1357850	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware 10.5.0 installed on FL MGUARD 4302 Order number: 1357840	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware 10.5.0 installed on FL MGUARD 4305 Order number: 1357875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware 10.5.0 installed on FL MGUARD 4102 PCIE Order number: 1357842	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware 10.5.0 installed on FL MGUARD 4102 PCI Order number: 1441187	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
OpenSSL 3.0.0	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9
OpenSSL 3.0.13	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9

First affected

Product	CVSS-Vector	CVSS Base Score
OpenSSL 3.0.0	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9

Last affected

Product	CVSS-Vector	CVSS Base Score
OpenSSL 3.0.13	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Fixed

Product
Firmware 10.6.0 installed on FL MGUARD 2102 Order number: 1357828 (Download)
Firmware 10.6.0 installed on FL MGUARD 2105 Order number: 1357850 (Download)
Firmware 10.6.0 installed on FL MGUARD 4302 Order number: 1357840 (Download)
Firmware 10.6.0 installed on FL MGUARD 4305 Order number: 1357875 (Download)
Firmware 10.6.0 installed on FL MGUARD 4102 PCIE Order number: 1357842 (Download)
Firmware 10.6.0 installed on FL MGUARD 4102 PCI Order number: 1441187 (Download)
OpenSSL 3.0.14

Acknowledgments

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

- CERT@VDE for coordination (see: https://certvde.com)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025-00024 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact
- VDE-2025-109: Phoenix Contact: Unbounded growth of the session cache in TCP encapsulation service in FL MGUARD 2xxx and 4xxx firmware - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-109
- VDE-2025-109: Phoenix Contact: Unbounded growth of the session cache in TCP encapsulation service in FL MGUARD 2xxx and 4xxx firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2025-109.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Tue Feb 10 09:00:00 CET 2026	Initial release.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany