TLP:WHITE

VDE-2025-077: Phoenix Contact: Two vulnerabilities in the jq JSON processor utilized by FL MGUARD 110x devices

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Sep 09 12:00:00 CEST 2025	Engine: 2.5.32
Current release date: Tue Sep 09 12:00:00 CEST 2025	Build Date: Thu Aug 28 11:27:08 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 7.5	Severity: MEDIUM
Original language: en	Language: en-US
Also referred to: VDE-2025-077, PCSA-2025/00016	

Summary

The jq JSON processor, which is used to migrate firmware configurations in the product, contains 2 vulnerabilities that can be exploited by an authenticated attacker.

General Recommendation

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

Impact

An authenticated attacker can cause a denial of service.

Remediation

Phoenix Contact strongly recommends upgrading affected mGuard devices to firmware version 1.8.1 or higher which fixes this vulnerability.

Product Description

mGuards are industrial routers and security appliances.

Product groups

Affected products

- Firmware <1.8.1 installed on FL MGUARD 1102
- Firmware <1.8.1 installed on FL MGUARD 1105

Fixed products

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

- Firmware 1.8.1 installed on FL MGUARD 1102
- Firmware 1.8.1 installed on FL MGUARD 1105

Vulnerabilities

CVE-2024-23337

Vulnerability Characterization

An authenticated attacker can cause a denial of service (memory exhaustion) by sending malformed data to the device in an HTTPS request. The impact is mitigated by the device enforcing a limit to the maximum HTTPS request size. To launch a successful attack, an attacker would have to circumvent this limit.

Vulnerability Details

In FL MGUARD devices, the jq JSON processor is used to migrate firmware configurations. The vulnerability can only be exploited by an authenticated administrative user in FL MGUARD devices. This reduces the vulnerability's severity to: CVSS-Score: 4.9, CSSS-Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Vulnerability Description

jq is a command-line JSON processor. In versions up to and including 1.7.1, an integer overflow arises when assigning value using an index of 2147483647, the signed integer limit. This causes a denial of service. Commit de21386681c0df0104a99d9d09db23a9b2a78b1e contains a patch for the issue.

CWE: CWE-190: Integer Overflow or Wraparound

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <1.8.1 installed on FL MGUARD 1102 Order number: 1153079	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	6.5
Firmware <1.8.1 installed on FL MGUARD 1105 Order number: 1153078	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 1.8.1 installed on FL MGUARD 1102 Order number: 1153079 (Download)
Firmware 1.8.1 installed on FL MGUARD 1105 Order number: 1153078 (Download)

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

CVE-2025-48060

Vulnerability Characterization

An authenticated attacker can cause a denial of service (crash of HTTPS request processor) by sending malformed data to the device in an HTTPS request.

Vulnerability Details

In FL MGUARD devices, the jq JSON processor is used to migrate firmware configurations. The vulnerability can only be exploited by an authenticated administrative user in FL MGUARD devices. This reduces the vulnerability's severity to: CVSS-Score: 4.9, CSSS-Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N /S:U/C:N/I:N/A:H

Vulnerability Description

jq is a command-line JSON processor. In versions up to and including 1.7.1, a heap-buffer-overflow is present in function `jv_string_vfmt` in the jq_fuzz_execute harness from oss-fuzz. This crash happens on file jv.c, line 1456 `void* p = malloc(sz);`. As of time of publication, no patched versions are available.

CWE: CWE-787: Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <1.8.1 installed on FL MGUARD 1102 Order number: 1153079	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <1.8.1 installed on FL MGUARD 1105 Order number: 1153078	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 1.8.1 installed on FL MGUARD 1102 Order number: 1153079 (Download)
Firmware 1.8.1 installed on FL MGUARD 1105 Order number: 1153078 (Download)

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
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025/00016 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2025-077: Phoenix Contact: Two vulnerabilities in the jq JSON processor utilized by FL MGUARD 110x devices - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-077
- VDE-2025-077: Phoenix Contact: Two vulnerabilities in the jq JSON processor utilized by FL MGUARD 110x devices - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-077.json

Revision history

Version	Date of the revision	Summary of the revision
1	Mon Aug 04 12:00:00 CEST 2025	Initial revision.

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