

SE-SA-2026_001: SE-Elektronic Security Advisory: Firmware V03.07.03 - Multiple Vulnerabilities (CVE-2024-1014, CVE-2024-1015)

Publisher: SE-Elektronic GmbH

Initial release date: 2026-07-16T22:00:00.000Z

Current release date: 2026-08-27T22:00:00.000Z

Current version: 3

CVSSv3.1 Base Score: 9.8

Original language:

Also referred to:

Document category: csaf_security_advisory

Engine: Secvisogram 2.6.5-1-g2d5db35f

Build Date: 2026-08-28T05:09:59.296Z

Status: final

Severity: CRITICAL

Language: en-GB

Summary

This advisory addresses multiple vulnerabilities in Firmware V03.07.03 and later.

Impact

This advisory addresses two vulnerabilities. Successful exploitation allows attackers to either execute arbitrary code, potentially compromising the device entirely, or trigger a Denial of Service (DoS) condition that causes the system to crash.

Remediation

Customers should update the firmware to version V03.08.52 or later. For latest firmware-version please contact support@se-elektronic.com

Vulnerabilities

(CVE-2024-1014)

Summary

Uncontrolled resource consumption vulnerability in Firmware versions 03.07.03 and higher. An attacker could interrupt the availability of the administration panel by sending multiple ICMP packets.

CWE: CWE-400:Uncontrolled Resource Consumption

Release date: 2024-01-28T23:00:00.000Z

Product status

Known affected

Product	CVSS-Vector	CVSS Score	Base
FW V03.08.18 installed on PLC I4.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.18 installed on E-DDC9.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.08 installed on E-DDC FG01	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.08 installed on E-DDC2.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.27 installed on E-DDC FG11	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.27 installed on E-DDC FG12	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.09 installed on E-DDC6.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.09 installed on E-DDC6.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.09 installed on E-DDC7.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.06 installed on X-RUS3.1 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.06 installed on E-DDC-A4.2	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.06 installed on E-DDC-A4.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.31 installed on E-DDC 13	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.05 installed on UGW-C	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.05 installed on X-RUS3.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.05 installed on X-RUS3.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.05 installed on X-RUS3.0 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on XRUS2.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.2	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.0 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.2 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on ROUTER-BC	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on GW-BC-SE	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	

Product	CVSS-Vector	CVSS Score	Base
FW V03.07.03 installed on UGW S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on UGW	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.3 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.3 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.4	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC5.4 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.4 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on RMAS	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B5.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B5.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B6.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B6.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B9.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC-B9.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC3.4	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on ROUTER-GSM TH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on ROUTER-GSM T	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC4.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.07.03 installed on E-DDC4.0 S	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.30 installed on M-DDC1.3	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.30 installed on E-DDC FG13	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.26 installed on M-DDC1.0	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	
FW V03.08.26 installed on M-DDC1.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	6.2	

Remediations

Vendor fix (2026-01-27T23:00:00.000Z)

Update the firmware of the affected devices to version V03.08.52 or later.

For products:

- FW V03.08.27 installed on E-DDC FG11
- FW V03.08.27 installed on E-DDC FG12
- FW V03.08.31 installed on E-DDC 13
- FW V03.08.30 installed on M-DDC1.3
- FW V03.08.30 installed on E-DDC FG13
- FW V03.08.26 installed on M-DDC1.0
- FW V03.08.26 installed on M-DDC1.1

<https://www.se-elektronik.com/support/>

Restart required: **none**

Device will restart automatically after firmware-update

None available

The affected product versions do not support the firmware version that contains the security fix. As these products have reached End of Support (EOS), no further security updates or remediation will be made available. Customers should transition to a supported hardware generation.

For products:

- FW V03.08.18 installed on PLC I4.0
- FW V03.08.18 installed on E-DDC9.0
- FW V03.08.08 installed on E-DDC FG01
- FW V03.08.08 installed on E-DDC2.3
- FW V03.07.09 installed on E-DDC6.0
- FW V03.07.09 installed on E-DDC6.3
- FW V03.07.09 installed on E-DDC7.3
- FW V03.07.06 installed on X-RUS3.1 S
- FW V03.07.06 installed on E-DDC-A4.2
- FW V03.07.06 installed on E-DDC-A4.3
- FW V03.07.05 installed on UGW-C
- FW V03.07.05 installed on X-RUS3.0
- FW V03.07.05 installed on X-RUS3.1
- FW V03.07.05 installed on X-RUS3.0 S
- FW V03.07.03 installed on XRUS2.1
- FW V03.07.03 installed on E-DDC3.2
- FW V03.07.03 installed on E-DDC5.0
- FW V03.07.03 installed on E-DDC5.0 S
- FW V03.07.03 installed on E-DDC3.2 S
- FW V03.07.03 installed on ROUTER-BC
- FW V03.07.03 installed on GW-BC-SE
- FW V03.07.03 installed on UGW S
- FW V03.07.03 installed on UGW
- FW V03.07.03 installed on E-DDC5.3
- FW V03.07.03 installed on E-DDC5.3 S
- FW V03.07.03 installed on E-DDC3.3 S

- FW V03.07.03 installed on E-DDC5.4
- FW V03.07.03 installed on E-DDC5.4 S
- FW V03.07.03 installed on E-DDC3.4 S
- FW V03.07.03 installed on RMAS
- FW V03.07.03 installed on E-DDC-B5.0
- FW V03.07.03 installed on E-DDC-B5.1
- FW V03.07.03 installed on E-DDC-B6.0
- FW V03.07.03 installed on E-DDC-B6.1
- FW V03.07.03 installed on E-DDC-B9.0
- FW V03.07.03 installed on E-DDC-B9.1
- FW V03.07.03 installed on E-DDC3.3
- FW V03.07.03 installed on E-DDC3.4
- FW V03.07.03 installed on ROUTER-GSM TH
- FW V03.07.03 installed on ROUTER-GSM T
- FW V03.07.03 installed on E-DDC4.0
- FW V03.07.03 installed on E-DDC4.0 S

(CVE-2024-1015)

Summary

Remote command execution vulnerability in firmware versions 03.07.03 and higher. An attacker could send different commands from the operating system to the system via the web configuration functionality of the device.

CWE: CWE-94:Improper Control of Generation of Code ('Code Injection')
Release date: 2024-01-28T23:00:00.000Z

Product status

Known affected

Product	CVSS-Vector	CVSS Score	Base
FW V03.08.18 installed on PLC I4.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.18 installed on E-DDC9.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.08 installed on E-DDC FG01	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.08 installed on E-DDC2.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.27 installed on E-DDC FG11	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.27 installed on E-DDC FG12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.09 installed on E-DDC6.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.09 installed on E-DDC6.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.09 installed on E-DDC7.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	

Product	CVSS-Vector	CVSS Score	Base
FW V03.07.06 installed on X-RUS3.1 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.06 installed on E-DDC-A4.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.06 installed on E-DDC-A4.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.31 installed on E-DDC 13	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.05 installed on UGW-C	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.05 installed on X-RUS3.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.05 installed on X-RUS3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.05 installed on X-RUS3.0 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on XRUS2.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.0 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.2 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on ROUTER-BC	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on GW-BC-SE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on UGW S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on UGW	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.3 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.3 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.4	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC5.4 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.4 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on RMAS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC-B5.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	

Product	CVSS-Vector	CVSS Score	Base
FW V03.07.03 installed on E-DDC-B5.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC-B6.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC-B6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC-B9.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC-B9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC3.4	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on ROUTER-GSM TH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on ROUTER-GSM T	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC4.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.07.03 installed on E-DDC4.0 S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.30 installed on M-DDC1.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.30 installed on E-DDC FG13	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.26 installed on M-DDC1.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	
FW V03.08.26 installed on M-DDC1.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	

Remediations

Vendor fix (2026-01-27T23:00:00.000Z)

Update the firmware of the affected devices to version V03.08.52 or later.

For products:

- FW V03.08.27 installed on E-DDC FG11
- FW V03.08.27 installed on E-DDC FG12
- FW V03.08.31 installed on E-DDC 13
- FW V03.08.30 installed on M-DDC1.3
- FW V03.08.30 installed on E-DDC FG13
- FW V03.08.26 installed on M-DDC1.0
- FW V03.08.26 installed on M-DDC1.1

<https://www.se-elektronik.com/support/>

Restart required: **none**

Device will restart automatically after firmware-update

None available

This product version on these specific hardware models has reached End of Support (EOS). No security updates will be provided. Users are advised to transition to a supported hardware generation.

For products:

- FW V03.08.18 installed on PLC I4.0
- FW V03.08.18 installed on E-DDC9.0
- FW V03.08.08 installed on E-DDC FG01
- FW V03.08.08 installed on E-DDC2.3
- FW V03.07.09 installed on E-DDC6.0
- FW V03.07.09 installed on E-DDC6.3
- FW V03.07.09 installed on E-DDC7.3
- FW V03.07.06 installed on X-RUS3.1 S
- FW V03.07.06 installed on E-DDC-A4.2
- FW V03.07.06 installed on E-DDC-A4.3
- FW V03.07.05 installed on UGW-C
- FW V03.07.05 installed on X-RUS3.0
- FW V03.07.05 installed on X-RUS3.1
- FW V03.07.05 installed on X-RUS3.0 S
- FW V03.07.03 installed on XRUS2.1
- FW V03.07.03 installed on E-DDC3.2
- FW V03.07.03 installed on E-DDC5.0
- FW V03.07.03 installed on E-DDC5.0 S
- FW V03.07.03 installed on E-DDC3.2 S
- FW V03.07.03 installed on ROUTER-BC
- FW V03.07.03 installed on GW-BC-SE
- FW V03.07.03 installed on UGW S
- FW V03.07.03 installed on UGW
- FW V03.07.03 installed on E-DDC5.3
- FW V03.07.03 installed on E-DDC5.3 S
- FW V03.07.03 installed on E-DDC3.3 S
- FW V03.07.03 installed on E-DDC5.4
- FW V03.07.03 installed on E-DDC5.4 S
- FW V03.07.03 installed on E-DDC3.4 S
- FW V03.07.03 installed on RMAS
- FW V03.07.03 installed on E-DDC-B5.0
- FW V03.07.03 installed on E-DDC-B5.1
- FW V03.07.03 installed on E-DDC-B6.0
- FW V03.07.03 installed on E-DDC-B6.1
- FW V03.07.03 installed on E-DDC-B9.0
- FW V03.07.03 installed on E-DDC-B9.1
- FW V03.07.03 installed on E-DDC3.3
- FW V03.07.03 installed on E-DDC3.4
- FW V03.07.03 installed on ROUTER-GSM TH
- FW V03.07.03 installed on ROUTER-GSM T
- FW V03.07.03 installed on E-DDC4.0
- FW V03.07.03 installed on E-DDC4.0 S

Acknowledgments

SE-Elektronik GmbH thanks the following parties for their efforts:

- Carlos Antonini from Spanish National Cybersecurity Institute, S.A (INCIBE) for Identified and responsibly disclosed the vulnerability.

SE-Elektronik GmbH

Namespace: <https://www.se-elektronik.com/psirt-cybersecurity>

psirt@se-elektronik.com

References

- Security Advisory SE-SA-2026_001 (self) https://www.se-elektronik.com/.well-known/csaf/advisories/2026/se-sa-2026_001.json

Revision history

Version	Date of the revision	Summary of the revision
1	2026-07-16T22:00:00.000Z	Publication Date
2	2026-07-30T10:00:00.000Z	Correction of the self-referencing link
3	2026-08-28T10:00:00.000Z	Correction of the Namespace of aggregate severity

Sharing rules

TLP:WHITE

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