Siemens Security Advisory by Siemens ProductCERT

SSA-674753: Denial-of-Service Vulnerability in ET 200 Devices

Publication Date:	2026-01-13
Last Update:	2026-02-10
Current Version:	V1.1
CVSS v3.1 Base Score:	7.5
CVSS v4.0 Base Score:	8.7

▼ SUMMARY

Siemens ET 200 devices contain a denial-of-service vulnerability that could be triggered by sending a valid S7 protocol Disconnect Request (COTP DR TPDU), causing the device to become unresponsive and require a power cycle to recover.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0) All versions affected by CVE-2025-40944	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (incl. SIPLUS variants)	Show more details
SIMATIC ET 200SP IM 155-6 MF HF (6ES7155-6MU00-0CN0) All versions affected by CVE-2025-40944	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants) All versions < V1.3 affected by CVE-2025-40944	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109987451/ See further recommendations from section Mitigations
SIMATIC ET 200SP IM 155-6 PN R1 (6ES7155-6AU00-0HM0) All versions < V6.0.1 affected by CVE-2025-40944	Update to V6.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109816000/ See further recommendations from section Mitigations
SIMATIC ET 200SP IM 155-6 PN/2 HF (incl. SIPLUS variants)	Show more details
SIMATIC ET 200SP IM 155-6 PN/3 HF (6ES7155-6AU30-0CN0) All versions < V4.2.2 affected by CVE-2025-40944	Update to V4.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109769419/

	See further recommendations from section Mitigations
SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0) All versions affected by CVE-2025-40944	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants)	Show more details

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- Filter the port 102 of the devices to only accepted connections to/from the IP addresses of machines that are trusted e.g. with an external firewall.
- Restrict access to the network where S7 communication messages are exchanged.

Product-specific remediations or mitigations can be found in the section Known Affected Products.
Please follow the General Security Recommendations.

▼ GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

▶ PRODUCT DESCRIPTION

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

▼ Vulnerability CVE-2025-40944

Affected devices do not properly handle S7 protocol session disconnect requests. When receiving a valid S7 protocol Disconnect Request (COTP DR TPDU) on TCP port 102, the devices enter an improper session state.

This could allow an attacker to cause the device to become unresponsive, leading to a denial-of-service condition that requires a power cycle to restore normal operation.

CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	8.7
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-400: Uncontrolled Resource Consumption

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Aitor Ruiz Larrea from Mytra Control for coordinated disclosure

▼ ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: https://www.siemens.com/cert/advisories

▼ HISTORY DATA

V1.0	(2026-01-13):	Publication Date
V1.1	(2026-02-10):	Added Researcher to Acknowledgements

▼ TERMS OF USE