



NCSC-2026-0005

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-01-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Siemens heeft kwetsbaarheden verholpen in diverse producten als Industrial Edge Devices, SCALANCE, SIMATIC, SIPLUS en Telecontrol Server.

Duiding

De kwetsbaarheden stellen een kwaadwillende mogelijk in staat aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- (Remote) code execution (root/admin rechten)
- Toegang tot systeemgegevens
- Verhogen van rechten

De kwaadwillende heeft hiervoor toegang nodig tot de productieomgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

Siemens heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Voor de kwetsbaarheden waar nog geen updates voor zijn, heeft Siemens mitigerende maatregelen gepubliceerd om de risico's zoveel als mogelijk te beperken. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- <https://cert-portal.siemens.com/productcert/html/ssa-001536.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-014678.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-192617.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-674753.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-827968.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-40805	10.0 CRITICAL

> CVE-2025-40891	2.3 LOW
> CVE-2025-40892	7.1 HIGH
> CVE-2025-40893	5.3 MEDIUM
> CVE-2025-40898	7.2 HIGH
> CVE-2025-40942	8.8 HIGH
> CVE-2025-40944	8.7 HIGH

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
> CWE-250	Execution with Unnecessary Privileges
> CWE-400	Uncontrolled Resource Consumption
> CWE-639	Authorization Bypass Through User-Controlled Key

Getroffen producten

Siemens
Industrial Edge Cloud Device (IECD)
Industrial Edge Device Kit - arm64 V1.10
Industrial Edge Device Kit - arm64 V1.11

Industrial Edge Device Kit - arm64 V1.12
Industrial Edge Device Kit - arm64 V1.13
Industrial Edge Device Kit - arm64 V1.14
Industrial Edge Device Kit - arm64 V1.15
Industrial Edge Device Kit - arm64 V1.16
Industrial Edge Device Kit - arm64 V1.17
Industrial Edge Device Kit - arm64 V1.18
Industrial Edge Device Kit - arm64 V1.19
Industrial Edge Device Kit - arm64 V1.20
Industrial Edge Device Kit - arm64 V1.21
Industrial Edge Device Kit - arm64 V1.22
Industrial Edge Device Kit - arm64 V1.23
Industrial Edge Device Kit - arm64 V1.24
Industrial Edge Device Kit - arm64 V1.25
Industrial Edge Device Kit - arm64 V1.5
Industrial Edge Device Kit - arm64 V1.6

Industrial Edge Device Kit - arm64 V1.7
Industrial Edge Device Kit - arm64 V1.8
Industrial Edge Device Kit - arm64 V1.9
Industrial Edge Device Kit - x86-64 V1.10
Industrial Edge Device Kit - x86-64 V1.11
Industrial Edge Device Kit - x86-64 V1.12
Industrial Edge Device Kit - x86-64 V1.13
Industrial Edge Device Kit - x86-64 V1.14
Industrial Edge Device Kit - x86-64 V1.15
Industrial Edge Device Kit - x86-64 V1.16
Industrial Edge Device Kit - x86-64 V1.17
Industrial Edge Device Kit - x86-64 V1.18
Industrial Edge Device Kit - x86-64 V1.19
Industrial Edge Device Kit - x86-64 V1.20
Industrial Edge Device Kit - x86-64 V1.21
Industrial Edge Device Kit - x86-64 V1.22

Industrial Edge Device Kit - x86-64 V1.23
Industrial Edge Device Kit - x86-64 V1.24
Industrial Edge Device Kit - x86-64 V1.25
Industrial Edge Device Kit - x86-64 V1.5
Industrial Edge Device Kit - x86-64 V1.6
Industrial Edge Device Kit - x86-64 V1.7
Industrial Edge Device Kit - x86-64 V1.8
Industrial Edge Device Kit - x86-64 V1.9
Industrial Edge Own Device (IEOD)
Industrial Edge Virtual Device (IEVD)
SCALANCE LPE9413
SCALANCE LPE9433
SIMATIC Automation Workstation 19"
SIMATIC Automation Workstation 24"
SIMATIC ET 200AL IM 157-1 PN
SIMATIC ET 200MP IM 155-5 PN HF

SIMATIC ET 200SP IM 155-6 MF HF
SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants)
SIMATIC ET 200SP IM 155-6 PN R1
SIMATIC ET 200SP IM 155-6 PN/2 HF
SIMATIC ET 200SP IM 155-6 PN/3 HF
SIMATIC HMI MTP1000 Unified Comfort Panel
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic neutral design
SIMATIC HMI MTP1000, Unified Comfort Panel neutral
SIMATIC HMI MTP1200 Comfort Pro for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1200 Comfort Pro for support arm (expandable, round tube) and extension unit
SIMATIC HMI MTP1200 Comfort Pro for support arm (not extendable, flange on top)
SIMATIC HMI MTP1200 Comfort Pro neutral design for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1200 Comfort Pro neutral design for support arm (expandable, round tube) and extensio
SIMATIC HMI MTP1200 Comfort Pro neutral design for support arm (not extendable, flange on top)
SIMATIC HMI MTP1200 Unified Comfort Panel

SIMATIC HMI MTP1200 Unified Comfort Panel hygienic
SIMATIC HMI MTP1200 Unified Comfort Panel hygienic neutral design
SIMATIC HMI MTP1200 Unified Comfort Panel neutral design
SIMATIC HMI MTP1500 Comfort Pro for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1500 Comfort Pro for support arm (expandable, round tube) and extension unit
SIMATIC HMI MTP1500 Comfort Pro for support arm (not extendable, flange on top)
SIMATIC HMI MTP1500 Comfort Pro neutral design for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1500 Comfort Pro neutral design for support arm (expandable, round tube) and extensio
SIMATIC HMI MTP1500 Comfort Pro neutral design for support arm (not extendable, flange on top)
SIMATIC HMI MTP1500 Unified Comfort Panel
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic neutral design
SIMATIC HMI MTP1500 Unified Comfort Panel neutral design
SIMATIC HMI MTP1900 Comfort Pro for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1900 Comfort Pro for support arm (expandable, round tube) and extension unit
SIMATIC HMI MTP1900 Comfort Pro for support arm (not extendable, flange on top)

SIMATIC HMI MTP1900 Comfort Pro neutral design for stand (expandable, flange at the bottom)
SIMATIC HMI MTP1900 Comfort Pro neutral design for support arm (expandable, round tube) and extensio
SIMATIC HMI MTP1900 Comfort Pro neutral design for support arm (not extendable, flange on top)
SIMATIC HMI MTP1900 Unified Comfort Panel
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic neutral design
SIMATIC HMI MTP1900 Unified Comfort Panel neutral design
SIMATIC HMI MTP2200 Comfort Pro for stand (expandable, flange at the bottom)
SIMATIC HMI MTP2200 Comfort Pro for support arm (expandable, round tube) and extension unit
SIMATIC HMI MTP2200 Comfort Pro for support arm (not extendable, flange on top)
SIMATIC HMI MTP2200 Comfort Pro neutral design for stand (expandable, flange at the bottom)
SIMATIC HMI MTP2200 Comfort Pro neutral design for support arm (expandable, round tube) and extensio
SIMATIC HMI MTP2200 Comfort Pro neutral design for support arm (not extendable, flange on top)
SIMATIC HMI MTP2200 Unified Comfort Hygienic
SIMATIC HMI MTP2200 Unified Comfort Hygienic neutral design
SIMATIC HMI MTP2200 Unified Comfort Panel

SIMATIC HMI MTP2200 Unified Comfort Panel neutral design
SIMATIC HMI MTP700 Unified Comfort Panel hygienic neutral design
SIMATIC HMI MTP700, Unified Comfort Panel neutral design
SIMATIC HMI MTP700 Unified Comfort Panel
SIMATIC IOT2050
SIMATIC IPC BX-39A Industrial Edge Device
SIMATIC IPC BX-59A Industrial Edge Device
SIMATIC IPC127E Industrial Edge Device
SIMATIC IPC227E Industrial Edge Device
SIMATIC IPC227G Industrial Edge Device
SIMATIC IPC427E Industrial Edge Device
SIMATIC IPC847E Industrial Edge Device
SIMATIC PN/MF Coupler
SIMATIC PN/PN Coupler
SIPLUS ET 200MP IM 155-5 PN HF
SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL

SIPLUS ET 200SP IM 155-6 PN HF
SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL
SIPLUS ET 200SP IM 155-6 PN HF TX RAIL
SIPLUS HMI MTP1000 Unified Comfort
SIPLUS HMI MTP1200 Unified Comfort
SIPLUS HMI MTP700 Unified Comfort
SIPLUS NET PN/PN Coupler
TeleControl Server Basic

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.