Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0077

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-03-2025

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 SCALANCE, SIMATIC, SINAMICS, SINEMA, SiPass, Teamcenter en Tecnomatix.

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
- Omzeilen van authenticatie
- (Remote) code execution (root/admin rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens
- Spoofing

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.

Dreigingsinformatie

Referenties

- https://cert-portal.siemens.com/productcert/pdf/ssa-050438.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-073066.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-075201.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-216014.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-280834.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-503939.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-507653.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-515903.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-615740.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-787280.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-858251.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-1305	9.8 CRITICAL
CVE-2024-4877	
CVE-2024-5594	9.1 CRITICAL
CVE-2024-24974	7.5 HIGH
CVE-2024-27459	7.8 HIGH
CVE-2024-27903	9.8 CRITICAL
CVE-2024-28882	6.5 MEDIUM
CVE-2024-41046	7.8 HIGH
CVE-2024-41049	7.8 HIGH
CVE-2024-41055	5.5 MEDIUM
CVE-2024-42154	4.4 MEDIUM
CVE-2024-42161	5.1 MEDIUM
CVE-2024-42512	8.6 HIGH
CVE-2024-42513	6.5 MEDIUM
CVE-2024-52285	6.9 MEDIUM
CVE-2024-56181	9.3 CRITICAL
CVE-2024-56182	9.3 CRITICAL
CVE-2024-56336	9.5 CRITICAL

CVE-2025-23384	6.3 MEDIUM
CVE-2025-23396	7.3 HIGH
CVE-2025-23397	7.3 HIGH
CVE-2025-23398	7.3 HIGH
CVE-2025-23399	7.3 HIGH
CVE-2025-23400	7.3 HIGH
CVE-2025-23401	7.3 HIGH
CVE-2025-23402	7.3 HIGH
CVE-2025-25266	7.0 HIGH
CVE-2025-25267	6.9 MEDIUM
CVE-2025-27392	8.6 HIGH
CVE-2025-27393	8.6 HIGH
CVE-2025-27394	8.6 HIGH
CVE-2025-27395	8.6 HIGH
CVE-2025-27396	8.7 HIGH
CVE-2025-27397	5.1 MEDIUM
CVE-2025-27398	2.1 LOW
CVE-2025-27438	7.3 HIGH
CVE-2025-27493	9.4 CRITICAL
CVE-2025-27494	9.4 CRITICAL

CWE's

CWE	Beschrijving
CWE-187	Partial String Comparison
CWE-283	Unverified Ownership
CWE-273	Improper Check for Dropped Privileges
CWE-1287	Improper Validation of Specified Type of Input
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-208	Observable Timing Discrepancy
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-824	Access of Uninitialized Pointer
CWE-305	Authentication Bypass by Primary Weakness
CWE-117	Improper Output Neutralization for Logs
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-190	Integer Overflow or Wraparound
CWE-693	Protection Mechanism Failure
CWE-552	Files or Directories Accessible to External Parties
CWE-290	Authentication Bypass by Spoofing
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-125	Out-of-bounds Read
CWE-306	Missing Authentication for Critical Function
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference

CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-787	Out-of-bounds Write
CWE-121	Stack-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-287	Improper Authentication

Getroffen producten

Siemens
RUGGEDCOM RM1224 LTE(4G) EU
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2)
RUGGEDCOM RM1224 LTE(4G) NAM
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2)
SCALANCE LPE9403
SCALANCE M804PB
SCALANCE M804PB (6GK5804-0AP00-2AA2)
SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2)
SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2)

SCALANCE M812-1 ADSL- Router family
SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2)
SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2)
SCALANCE M816-1 ADSL- Router family
SCALANCE M826-2 SHDSL-Router
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2)
SCALANCE M874-2
SCALANCE M874-2 (6GK5874-2AA00-2AA2)
SCALANCE M874-3
SCALANCE M874-3 (6GK5874-3AA00-2AA2)
SCALANCE M874-3 3G- Router (CN)
SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2)
SCALANCE M876-3
SCALANCE M876-3 (6GK5876-3AA02-2BA2)
SCALANCE M876-3 (ROK)
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2)

SCALANCE M876-4
SCALANCE M876-4 (6GK5876-4AA10-2BA2)
SCALANCE M876-4 (EU)
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2)
SCALANCE M876-4 (NAM)
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2)
SCALANCE MUB852-1 (A1)
SCALANCE MUB852-1 (B1)
SCALANCE MUM853-1 (A1)
SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1)
SCALANCE MUM853-1 (B1)
SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1)
SCALANCE MUM853-1 (EU)
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1)
SCALANCE MUM856-1 (A1)
SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1)

SCALANCE MUM856-1 (B1)
SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1)
SCALANCE MUM856-1 (CN)
SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1)
SCALANCE MUM856-1 (EU)
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1)
SCALANCE MUM856-1 (RoW)
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1)
SCALANCE S615 EEC LAN-Router
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2)
SCALANCE S615 LAN- Router
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2)
SCALANCE SC-600 family
SIMATIC Field PG M5
SIMATIC Field PG M6
SIMATIC IPC BX-21A

SIMATIC IPC BX-32A
SIMATIC IPC BX-39A
SIMATIC IPC BX-59A
SIMATIC IPC PX-32A
SIMATIC IPC PX-39A
SIMATIC IPC PX-39A PRO
SIMATIC IPC RC-543B
SIMATIC IPC RW-543A
SIMATIC IPC127E
SIMATIC IPC227E
SIMATIC IPC227G
SIMATIC IPC277E
SIMATIC IPC277G
SIMATIC IPC3000 SMART V3
SIMATIC IPC327G
SIMATIC IPC347G

SIMATIC IPC377G
SIMATIC IPC427E
SIMATIC IPC477E
SIMATIC IPC477E PRO
SIMATIC IPC527G
SIMATIC IPC627E
SIMATIC IPC647E
SIMATIC IPC677E
SIMATIC IPC847E
SIMATIC ITP1000
SIMATIC IPC277G PRO
SINAMICS S200
SiPass integrated AC5102 (ACC-G2)
SiPass integrated AC5102, SiPass integrated ACC-AP
SiPass integrated ACC-AP
Teamcenter Visualization V14.3

Teamcenter Visualization V2312
Teamcenter Visualization V2406
Teamcenter Visualization V2412
Tecnomatix Plant Simulation V2302
Tecnomatix Plant Simulation V2404

Disclaimer