Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0112

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-04-2026

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 zoals Analytics Toolkit, Ruggedcom, Industrial Edge Management Pro, SIDIS en TPM.

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

Voor succesvol misbruik van de genoemde kwetsbaarheden moet de kwaadwillende toegang hebben tot de productie-omgeving. 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-019200.html
- https://cert-portal.siemens.com/productcert/html/ssa-225816.html
- https://cert-portal.siemens.com/productcert/html/ssa-605717.html
- https://cert-portal.siemens.com/productcert/html/ssa-609469.html
- https://cert-portal.siemens.com/productcert/html/ssa-628843.html
- https://cert-portal.siemens.com/productcert/html/ssa-741509.html
- https://cert-portal.siemens.com/productcert/html/ssa-801704.html
- https://cert-portal.siemens.com/productcert/html/ssa-981622.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-24588	6.5 MEDIUM
CVE-2020-26139	5.3 MEDIUM
CVE-2020-26140	6.5 MEDIUM
CVE-2020-26141	6.5 MEDIUM
CVE-2020-26143	6.5 MEDIUM
CVE-2020-26144	6.5 MEDIUM
CVE-2020-26146	5.3 MEDIUM
CVE-2020-26147	5.4 MEDIUM
CVE-2021-3712	7.4 HIGH
CVE-2022-0778	7.5 HIGH
CVE-2022-31765	8.8 HIGH
CVE-2022-36323	9.1 CRITICAL
CVE-2022-36324	7.5 HIGH
CVE-2022-36325	6.8 MEDIUM
CVE-2023-44373	9.4 CRITICAL
CVE-2025-2884	6.6 MEDIUM
CVE-2025-6965	7.2 HIGH
CVE-2025-40745	6.3 MEDIUM
CVE-2026-24032	6.9 MEDIUM
CVE-2026-25654	8.7 HIGH
CVE-2026-27668	8.7 HIGH

CVE-2026-33892	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
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-99	Improper Control of Resource Identifiers ('Resource Injection')
CWE-125	Out-of-bounds Read
CWE-197	Numeric Truncation Error
CWE-266	Incorrect Privilege Assignment
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-290	Authentication Bypass by Spoofing
CWE-295	Improper Certificate Validation
CWE-305	Authentication Bypass by Primary Weakness
CWE-306	Missing Authentication for Critical Function
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-345	Insufficient Verification of Data Authenticity
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
CWE-354	Improper Validation of Integrity Check Value

CWE-400	Uncontrolled Resource Consumption
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

Getroffen producten

Siemens
6AG1206-2BB00-7AC2 Firmware
6Ag1206-2Bs00-7Ac2 Firmware
6Ag1208-0Ba00-7Ac2 Firmware
6Ag1216-4Bs00-7Ac2 Firmware
6GK5204-0BA00-2GF2 Firmware
6GK5204-0BA00-2YF2 Firmware
6GK5205-3BB00-2AB2 FIRMWARE
6GK5205-3BB00-2AB2 Firmware
6GK5205-3BB00-2TB2 Firmware

6GK5205-3BF00-2TB2 FIRMWARE
6GK5206-2BD00-2AC2 Firmware
6GK5206-2GS00-2AC2 Firmware
6GK5206-2GS00-2TC2 Firmware
6GK5206-2RS00-2AC2 Firmware
6GK5208-0BA00-2AB2 Firmware
6GK5208-0BA00-2AC2 Firmware
6GK5208-0BA00-2FC2 Firmware
6GK5208-0GA00-2AC2 Firmware
6GK5208-0GA00-2FC2 Firmware
6GK5208-0GA00-2TC2 Firmware
6GK5632-2GS00-2AC2 FIRMWARE
6GK5646-2GS00-2AC2 FIRMWARE
6GK5721-1FC00-0AB0 FIRMWARE
6GK5722-1FC00-0AB0 FIRMWARE
6GK5734-1FX00-0AA0 FIRMWARE
BFCClient

CP 1243-1 Firmware (OS)
CP 1243-7 LTE EU Firmware (OS)
CP 1243-7 LTE US Firmware (OS)
CP 1243-8 IRC Firmware (OS)
CP 1542SP-1 Firmware (OS)
Industrial Edge - Machine Insight App
Industrial Edge - OPC UA Connector
Industrial Edge - Opc Ua Connector
Industrial Edge - PROFINET IO Connector
Industrial Edge - SIMATIC S7 Connector App
Industrial Edge - Simatic S7 Connector App
Industrial Edge Management
Industrial Edge Management Pro V1
Industrial Edge Management Pro V2
Industrial Edge Management Virtual
Open PCS 7

OpenPCS 7 V8.2
OpenPCS 7 V9.0
OpenPCS 7 V9.1
ROX II Firmware
RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P)
RUGGEDCOM CROSSBOW Station Access Controller (SAC)
RUGGEDCOM RM1224 Firmware
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)
RUGGEDCOM RM1224 LTE4G
RUGGEDCOM ROX MX5000
RUGGEDCOM ROX MX5000RE
RUGGEDCOM ROX RX1400
RUGGEDCOM ROX RX1500

RUGGEDCOM ROX RX1500 FIRMWARE
RUGGEDCOM ROX RX1501
RUGGEDCOM ROX RX1510
RUGGEDCOM ROX RX1510 FIRMWARE
RUGGEDCOM ROX RX1511
RUGGEDCOM ROX RX1512
RUGGEDCOM ROX RX1524
RUGGEDCOM ROX RX1524 (Hardware)
RUGGEDCOM ROX RX1536
RUGGEDCOM ROX RX5000
RUGGEDCOM RX1400 (Firmware)
Ruggedcom Rm1224 Lte Eu
Ruggedcom Rm1224 Lte Nam
Ruggedcom Rox Mx5000
Ruggedcom Rox Rx1500
Ruggedcom Rox Rx1501

Ruggedcom Rox Rx1512
SCALANCE M816-1 (Hardware)
SCALANCE M826-2 (Hardware)
SCALANCE M874-2 (Hardware)
SCALANCE M876-3 (Hardware)
SCALANCE M876-4 (Hardware)
SCALANCE MUM856-1 (Hardware)
SCALANCE S615
SCALANCE SC-600 Firmware
SCALANCE SC622-2C

Disclaimer