Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0106

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-04-2025

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 Industrial Edge Devices, Mendix, SENTRON, SIDIS, SIMATIC, SIPLUS,Insights Hub Private Cloud, Siemens License Server en Solid Edge.

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-187636.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-277137.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-525431.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-634640.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-672923.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-725549.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-819629.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-874353.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-817234.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-21658	7.3 HIGH
CVE-2023-2975	7.8 HIGH
CVE-2023-3446	7.8 HIGH
CVE-2023-3817	7.8 HIGH
CVE-2023-4807	7.8 HIGH
CVE-2023-5363	7.5 HIGH
CVE-2023-5678	
CVE-2023-7104	7.3 HIGH
CVE-2024-0056	8.7 HIGH
CVE-2024-0232	
CVE-2024-0727	7.5 HIGH
CVE-2024-5535	9.1 CRITICAL
CVE-2024-9143	6.9 MEDIUM
CVE-2024-21319	
CVE-2024-23814	6.9 MEDIUM
CVE-2024-30105	7.5 HIGH
CVE-2024-41788	9.4 CRITICAL
CVE-2024-41789	9.4 CRITICAL
CVE-2024-41790	9.4 CRITICAL

CVE-2024-41791	6.9 MEDIUM
CVE-2024-41792	9.2 CRITICAL
CVE-2024-41793	7.7 HIGH
CVE-2024-41794	10.0 CRITICAL
CVE-2024-41795	6.9 MEDIUM
CVE-2024-41796	6.9 MEDIUM
CVE-2024-54091	8.7 HIGH
CVE-2024-54092	9.3 CRITICAL
CVE-2025-30280	6.9 MEDIUM
CVE-2025-1097	8.8 HIGH
CVE-2025-24514	8.8 HIGH
CVE-2025-24513	4.8 MEDIUM
CVE-2025-1974	9.8 CRITICAL
CVE-2025-1098	8.8 HIGH
CVE-2025-29999	7.3 HIGH
CVE-2025-30000	5.4 MEDIUM

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-606	Unchecked Input for Loop Condition
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-363	Race Condition Enabling Link Following

CWE-420	Unprotected Alternate Channel
CWE-684	Incorrect Provision of Specified Functionality
CWE-834	Excessive Iteration
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-440	Expected Behavior Violation
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-319	Cleartext Transmission of Sensitive Information
CWE-354	Improper Validation of Integrity Check Value
CWE-325	Missing Cryptographic Step
CWE-404	Improper Resource Shutdown or Release
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-400	Uncontrolled Resource Consumption
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-1390	Weak Authentication
CWE-204	Observable Response Discrepancy
CWE-15	External Control of System or Configuration Setting
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-653	Improper Isolation or Compartmentalization

CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-620	Unverified Password Change
CWE-798	Use of Hard-coded Credentials
CWE-269	Improper Privilege Management
CWE-295	Improper Certificate Validation

Getroffen producten

Siemens
Industrial Edge Own Device (IEOD)
Industrial Edge Device Kit - x86-64 V1.21
Industrial Edge Device Kit - x86-64 V1.20
Industrial Edge Device Kit - x86-64 V1.19
Industrial Edge Device Kit - x86-64 V1.18
Industrial Edge Device Kit - x86-64 V1.17
Industrial Edge Device Kit - arm64 V1.21
Industrial Edge Device Kit - arm64 V1.20
Industrial Edge Device Kit - arm64 V1.19
Industrial Edge Device Kit - arm64 V1.18
Industrial Edge Device Kit - arm64 V1.17

SENTRON 7KT PAC1260 Data Manager
License Server
Siemens License Server (SLS)
Solid Edge
Solid_Edge_Se2024
SINEC Network Management System
Siemens Simatic S7-1500 Tm Mfp
Siemens Telecontrol Server Basic
Solid Edge SE2024
Solid Edge SE2025
SIMATIC CFU DIQ
SIMATIC CFU PA
SIMATIC ET 200AL IM 157-1 PN
SIMATIC ET 200M IM 153-4 PN IO HF
SIMATIC ET 200M IM 153-4 PN IO ST
SIMATIC ET 200MP IM 155-5 PN BA

SIMATIC ET 200MP IM 155-5 PN HF
SIMATIC ET 200MP IM 155-5 PN ST
SIMATIC ET 200S IM 151-3 PN FO
SIMATIC ET 200S IM 151-3 PN HF
SIMATIC ET 200S IM 151-3 PN HS
SIMATIC ET 200S IM 151-3 PN ST
SIMATIC ET 200S IM 151-8 PN/DP CPU
SIMATIC ET 200S IM 151-8F PN/DP CPU
SIMATIC ET 200SP CPU 1510SP F-1 PN
SIMATIC ET 200SP CPU 1510SP-1 PN
SIMATIC ET 200SP CPU 1512SP F-1 PN
SIMATIC ET 200SP CPU 1512SP-1 PN
SIMATIC ET 200SP IM 155-6 MF HF
SIMATIC ET 200SP IM 155-6 PN BA
SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants)
SIMATIC ET 200SP IM 155-6 PN HF

SIMATIC ET 200SP IM 155-6 PN HS
SIMATIC ET 200SP IM 155-6 PN ST
SIDOOR ATD430W
SIDOOR ATE530G COATED
SIDOOR ATE530S COATED
SIMOCODE pro V Ethernet/IP (incl. SIPLUS variants)
SIMOCODE pro V PROFINET
SINUMERIK 840D sl
SIWAREX WP231
SIWAREX WP241
SIWAREX WP251
SIWAREX WP521 ST
SIWAREX WP522 ST
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants)
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)
SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants)

SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants)
SIPLUS ET 200M IM 153-4 PN IO HF
SIPLUS ET 200M IM 153-4 PN IO ST
SIPLUS ET 200MP IM 155-5 PN HF
SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL
SIPLUS ET 200MP IM 155-5 PN ST
SIPLUS ET 200MP IM 155-5 PN ST TX RAIL
SIPLUS ET 200S IM 151-8 PN/DP CPU
SIPLUS ET 200S IM 151-8F PN/DP CPU
SIPLUS ET 200S IM151-3 PN HF
SIPLUS ET 200S IM151-3 PN ST
SIPLUS ET 200SP CPU 1512SP F-1 PN
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 ET 200SP IM 155-6 PN ST

SIPLUS ET 200SP IM 155-6 PN ST BA
SIPLUS ET 200SP IM 155-6 PN ST BA TX RAIL
SIPLUS ET 200SP IM 155-6 PN ST TX RAIL
SIPLUS HCS4200 CIM4210
Mendix Runtime
Mendix Runtime V10
Mendix Runtime V10.12
Mendix Runtime V10.18
Mendix Runtime V10.6
Mendix Runtime V8
Mendix Runtime V9

Disclaimer