Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0187

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-06-2025

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 RUGGEDCOM, SCALANCE, SIMATIC 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.

Referenties

- https://cert-portal.siemens.com/productcert/pdf/ssa-082556.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-345750.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-486186.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-513708.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-633269.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-693776.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-41617	
CVE-2023-4527	7.8 HIGH
CVE-2023-4806	7.8 HIGH
CVE-2023-4911	7.8 HIGH
CVE-2023-5363	7.5 HIGH
CVE-2023-6246	8.4 HIGH
CVE-2023-6779	8.2 HIGH
CVE-2023-6780	7.8 HIGH
CVE-2023-28531	9.8 CRITICAL
CVE-2023-38545	9.8 CRITICAL
CVE-2023-38546	9.8 CRITICAL
CVE-2023-44487	6.9 MEDIUM
CVE-2023-46218	6.5 MEDIUM
CVE-2023-46219	9.8 CRITICAL
CVE-2023-48795	6.0 MEDIUM
CVE-2023-51384	5.9 MEDIUM
CVE-2023-51385	6.5 MEDIUM
CVE-2023-52927	5.1 MEDIUM
CVE-2024-2961	8.8 HIGH
CVE-2024-6119	9.1 CRITICAL
CVE-2024-6387	

CVE-2024-12133	6.9 MEDIUM
CVE-2024-12243	6.9 MEDIUM
CVE-2024-24855	5.1 MEDIUM
CVE-2024-26596	5.5 MEDIUM
CVE-2024-28085	8.8 HIGH
CVE-2024-33599	8.6 HIGH
CVE-2024-33600	8.6 HIGH
CVE-2024-33601	8.6 HIGH
CVE-2024-33602	8.6 HIGH
CVE-2024-34397	7.5 HIGH
CVE-2024-37370	9.1 CRITICAL
CVE-2024-37371	9.1 CRITICAL
CVE-2024-41797	4.3 MEDIUM
CVE-2024-45490	5.1 MEDIUM
CVE-2024-45491	5.1 MEDIUM
CVE-2024-45492	5.1 MEDIUM
CVE-2024-50246	5.1 MEDIUM
CVE-2024-53166	7.8 HIGH
CVE-2024-57977	5.5 MEDIUM
CVE-2024-57996	5.5 MEDIUM
CVE-2024-58005	5.5 MEDIUM
CVE-2025-0133	6.9 MEDIUM
CVE-2025-4373	5.1 MEDIUM

CVE-2025-4598	2.0 LOW
CVE-2025-21701	2.1 LOW
CVE-2025-21702	5.1 MEDIUM
CVE-2025-21712	5.5 MEDIUM
CVE-2025-21724	5.5 MEDIUM
CVE-2025-21728	5.1 MEDIUM
CVE-2025-21745	6.9 MEDIUM
CVE-2025-21756	8.6 HIGH
CVE-2025-21758	5.1 MEDIUM
CVE-2025-21765	5.5 MEDIUM
CVE-2025-21766	5.5 MEDIUM
CVE-2025-21767	5.1 MEDIUM
CVE-2025-21795	6.9 MEDIUM
CVE-2025-21796	
CVE-2025-21848	6.9 MEDIUM
CVE-2025-21862	2.1 LOW
CVE-2025-21864	5.1 MEDIUM
CVE-2025-21865	8.6 HIGH
CVE-2025-26465	6.3 MEDIUM
CVE-2025-31115	8.7 HIGH
CVE-2025-32454	7.3 HIGH
CVE-2025-40567	6.5 MEDIUM
CVE-2025-40568	4.3 MEDIUM

CVE-2025-40569	**4.8 MEDIUM**
CVE-2025-40585	**9.9 CRITICAL**
CVE-2025-46836	**6.6 MEDIUM**

CWE's

CWE	Beschrijving
CWE-395	Use of NullPointerException Catch to Detect NULL Pointer Dereference
CWE-332	Insufficient Entropy in PRNG
CWE-940	Improper Verification of Source of a Communication Channel
CWE-466	Return of Pointer Value Outside of Expected Range
CWE-390	Detection of Error Condition Without Action
CWE-826	Premature Release of Resource During Expected Lifetime
CWE-222	Truncation of Security-relevant Information
CWE-310	CWE-310
CWE-273	Improper Check for Dropped Privileges
CWE-364	Signal Handler Race Condition
CWE-911	Improper Update of Reference Count
CWE-131	Incorrect Calculation of Buffer Size
CWE-304	Missing Critical Step in Authentication
CWE-684	Incorrect Provision of Specified Functionality
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-268	Privilege Chaining
CWE-366	Race Condition within a Thread
CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences
CWE-201	Insertion of Sensitive Information Into Sent Data

CWE-407	Inefficient Algorithmic Complexity
CWE-371	CWE-371
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-667	Improper Locking
CWE-311	Missing Encryption of Sensitive Data
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-908	Use of Uninitialized Resource
CWE-617	Reachable Assertion
CWE-129	Improper Validation of Array Index
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-345	Insufficient Verification of Data Authenticity
CWE-354	Improper Validation of Integrity Check Value
CWE-325	Missing Cryptographic Step
CWE-190	Integer Overflow or Wraparound
CWE-290	Authentication Bypass by Spoofing
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')
CWE-665	Improper Initialization
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference

CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-611	Improper Restriction of XML External Entity Reference
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-73	External Control of File Name or Path
CWE-20	Improper Input Validation
CWE-863	Incorrect Authorization
CWE-276	Incorrect Default Permissions

Getroffen producten

Siemens
SIMATIC S7-1500
SIMATIC S7-1500 CPU 1518-4 PN/ DP MFP Firmware
Simatic S7-1500 Tm Mfp Firmware
RUGGEDCOM APE1808 Firmware

Ruggedcom Ape1808
Scalance W700 Ieee 802.11Ax Firmware
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0)
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AC0)
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0)
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AC0)
SIMATIC S7-1500 TM MFP - BIOS
SIMATIC S7-1500 TM MFP - GNU/ Linux subsystem
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0)
RUGGEDCOM APE1808
ruggedcom_ape1808
Energy Services
Tecnomatix Plant Simulation V2404
SCALANCE XC316-8 (6GK5324-8TS00-2AC2)
SCALANCE XC324-4 (6GK5328-4TS00-2AC2)
SCALANCE XC324-4 EEC (6GK5328-4TS00-2EC2)

SCALANCE XC332 (6GK5332-0GA00-2AC2)
SCALANCE XC416-8 (6GK5424-8TR00-2AC2)
SCALANCE XC424-4 (6GK5428-4TR00-2AC2)
SCALANCE XC432 (6GK5432-0GR00-2AC2)
SCALANCE XCH328 (6GK5328-4TS01-2EC2)
SCALANCE XCM324 (6GK5324-8TS01-2AC2)
SCALANCE XCM328 (6GK5328-4TS01-2AC2)
SCALANCE XCM332 (6GK5332-0GA01-2AC2)
SCALANCE XR302-32 (6GK5334-5TS00-2AR3)
SCALANCE XR302-32 (6GK5334-5TS00-3AR3)
SCALANCE XR302-32 (6GK5334-5TS00-4AR3)
SCALANCE XR322-12 (6GK5334-3TS00-2AR3)
SCALANCE XR322-12 (6GK5334-3TS00-3AR3)
SCALANCE XR322-12 (6GK5334-3TS00-4AR3)
SCALANCE XR326-8 (6GK5334-2TS00-2AR3)
SCALANCE XR326-8 (6GK5334-2TS00-3AR3)

SCALANCE XR326-8 (6GK5334-2TS00-4AR3)
SCALANCE XR326-8 EEC (6GK5334-2TS00-2ER3)
SCALANCE XR502-32 (6GK5534-5TR00-2AR3)
SCALANCE XR502-32 (6GK5534-5TR00-3AR3)
SCALANCE XR502-32 (6GK5534-5TR00-4AR3)
SCALANCE XR522-12 (6GK5534-3TR00-2AR3)
SCALANCE XR522-12 (6GK5534-3TR00-3AR3)
SCALANCE XR522-12 (6GK5534-3TR00-4AR3)
SCALANCE XR526-8 (6GK5534-2TR00-2AR3)
SCALANCE XR526-8 (6GK5534-2TR00-3AR3)
SCALANCE XR526-8 (6GK5534-2TR00-4AR3)
SCALANCE XRH334 (24 V DC, 8xFO, CC) (6GK5334-2TS01-2ER3)
SCALANCE XRM334 (230 V AC, 12xFO) (6GK5334-3TS01-3AR3)
SCALANCE XRM334 (230 V AC, 8xFO) (6GK5334-2TS01-3AR3)
SCALANCE XRM334 (230V AC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-3AR3)
SCALANCE XRM334 (24 V DC, 12xFO) (6GK5334-3TS01-2AR3)

SCALANCE XRM334 (24 V DC, 8xFO) (6GK5334-2TS01-2AR3)
SCALANCE XRM334 (24V DC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-2AR3)
SCALANCE XRM334 (2x230 V AC, 12xFO) (6GK5334-3TS01-4AR3)
SCALANCE XRM334 (2x230 V AC, 8xFO) (6GK5334-2TS01-4AR3)
SCALANCE XRM334 (2x230V AC, 2x10G, 24xSFP, 8xSFP+) (6GK5334-5TS01-4AR3)

Disclaimer