Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0079

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-03-2026

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 Heliox, Ruggedcom, SICAM, SIDIS en SIMATIC.

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-126399.html
- https://cert-portal.siemens.com/productcert/html/ssa-452276.html
- https://cert-portal.siemens.com/productcert/html/ssa-485750.html
- https://cert-portal.siemens.com/productcert/html/ssa-903736.html
- https://cert-portal.siemens.com/productcert/html/ssa-975644.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-29857	7.5 HIGH

CVE-2024-30171	7.5 HIGH
CVE-2024-30172	6.9 MEDIUM
CVE-2024-41996	6.3 MEDIUM
CVE-2025-6965	7.2 HIGH
CVE-2025-7783	9.4 CRITICAL
CVE-2025-9230	6.9 MEDIUM
CVE-2025-9232	6.3 MEDIUM
CVE-2025-9670	6.9 MEDIUM
CVE-2025-12816	8.7 HIGH
CVE-2025-15284	8.7 HIGH
CVE-2025-27769	2.6 LOW
CVE-2025-40943	9.6 CRITICAL
CVE-2025-55018	5.8 MEDIUM
CVE-2025-58751	6.3 MEDIUM
CVE-2025-58752	2.3 LOW
CVE-2025-58754	6.9 MEDIUM
CVE-2025-62439	4.2 MEDIUM
CVE-2025-62522	6.0 MEDIUM
CVE-2025-64157	6.7 MEDIUM
CVE-2025-64718	5.3 MEDIUM
CVE-2025-64756	7.5 HIGH
CVE-2025-66030	6.3 MEDIUM
CVE-2025-66031	8.7 HIGH

CVE-2025-66035	7.7 HIGH
CVE-2025-66412	8.5 HIGH
CVE-2025-69277	2.0 LOW
CVE-2026-22610	8.5 HIGH
CVE-2026-24858	9.8 CRITICAL
CVE-2026-25569	7.4 HIGH
CVE-2026-25570	7.4 HIGH
CVE-2026-25571	5.1 MEDIUM
CVE-2026-25572	5.1 MEDIUM
CVE-2026-25573	7.4 HIGH
CVE-2026-25605	6.7 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-73	External Control of File Name or Path
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-130	Improper Handling of Length Parameter Inconsistency

CWE-134	Use of Externally-Controlled Format String
CWE-179	Incorrect Behavior Order: Early Validation
CWE-184	Incomplete List of Disallowed Inputs
CWE-190	Integer Overflow or Wraparound
CWE-197	Numeric Truncation Error
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-203	Observable Discrepancy
CWE-208	Observable Timing Discrepancy
CWE-284	Improper Access Control
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-295	Improper Certificate Validation
CWE-330	Use of Insufficiently Random Values
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-436	Interpretation Conflict
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-674	Uncontrolled Recursion
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-937	CWE-937
CWE-940	Improper Verification of Source of a Communication Channel

CWE-1035	CWE-1035
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Siemens
Heliox Flex 180 kW EV Charging Station
Heliox Mobile DC 40 kW EV Charging Station
RUGGEDCOM APE1808
SICAM SIAPP SDK
SIDIS Prime
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0)
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0)
SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0)
SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0)
SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0)
SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DK03-0AB0)
SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0)

SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0)
SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DK01-0AB0)
SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DM03-0AB0)
SIMATIC ET 200SP CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0)
SIMATIC ET 200SP CPU 1514SP-2 PN (6ES7514-2DN03-0AB0)
SIMATIC ET 200SP CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0)
SIMATIC ET 200SP CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0)
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants)
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V2 CPUs - Windows OS
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Industrial OS
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Windows OS
SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V2 CPUs - Windows OS
SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V3 CPUs - Industrial OS
SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V3 CPUs - Windows OS
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK00-0AB0)
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0)

SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0)
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0)
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0)
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0)
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CL03-0AB0)
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0)
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0)
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0)
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0)
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TL03-0AB0)
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0)
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UL03-0AB0)
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0)
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0)
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CM03-0AB0)
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0)

SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0)
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0)
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0)
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0)
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0)
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0)
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RM03-0AB0)
SIMATIC S7-1500 CPU 1513pro F-2 PN (6ES7513-2GM03-0AB0)
SIMATIC S7-1500 CPU 1513pro-2 PN (6ES7513-2PM03-0AB0)
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0)
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0)
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AN03-0AB0)
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0)
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0)
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FN03-0AB0)
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0)

SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RN03-0AB0)
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0)
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TN03-0AB0)
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0)
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UN03-0AB0)
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0)
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0)
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AP03-0AB0)
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0)
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0)
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FP03-0AB0)
SIMATIC S7-1500 CPU 1516T-3 PN (6ES7516-3TP10-0AB0)
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0)
SIMATIC S7-1500 CPU 1516TF-3 PN (6ES7516-3UP10-0AB0)
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0)
SIMATIC S7-1500 CPU 1516pro F-2 PN (6ES7516-2GP03-0AB0)

SIMATIC S7-1500 CPU 1516pro-2 PN (6ES7516-2PP03-0AB0)
SIMATIC S7-1500 CPU 1517-3 PN (6ES7517-3AQ10-0AB0)
SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0)
SIMATIC S7-1500 CPU 1517F-3 PN (6ES7517-3FQ10-0AB0)
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0)
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP01-0AB0)
SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0)
SIMATIC S7-1500 CPU 1517H-4 PN (6ES7517-4HQ10-0AB0)
SIMATIC S7-1500 CPU 1517T-3 PN (6ES7517-3TQ10-0AB0)
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0)
SIMATIC S7-1500 CPU 1517TF-3 PN (6ES7517-3UQ10-0AB0)
SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0)
SIMATIC S7-1500 CPU 1518-3 PN (6ES7518-3AT10-0AB0)
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0)
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-3 PN (6ES7518-3FT10-0AB0)
SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0)
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 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0)
SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JT10-0AB0)
SIMATIC S7-1500 CPU 1518T-3 PN (6ES7518-3TT10-0AB0)
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0)
SIMATIC S7-1500 CPU 1518TF-3 PN (6ES7518-3UT10-0AB0)
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0)
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0)
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0)
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0)
SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0)
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0)
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0)

SIMATIC S7-1500 Software Controller CPU 1507S F V2
SIMATIC S7-1500 Software Controller CPU 1507S F V3
SIMATIC S7-1500 Software Controller CPU 1507S F V4
SIMATIC S7-1500 Software Controller CPU 1507S V2
SIMATIC S7-1500 Software Controller CPU 1507S V3
SIMATIC S7-1500 Software Controller CPU 1507S V4
SIMATIC S7-1500 Software Controller CPU 1508S F V2
SIMATIC S7-1500 Software Controller CPU 1508S F V3
SIMATIC S7-1500 Software Controller CPU 1508S F V4
SIMATIC S7-1500 Software Controller CPU 1508S T V3
SIMATIC S7-1500 Software Controller CPU 1508S TF V3
SIMATIC S7-1500 Software Controller CPU 1508S V2
SIMATIC S7-1500 Software Controller CPU 1508S V3
SIMATIC S7-1500 Software Controller CPU 1508S V4
SIMATIC S7-1500 Software Controller Linux V2
SIMATIC S7-1500 Software Controller Linux V3

SIMATIC S7-1500 TM MFP - GNU/ Linux subsystem
SIMATIC S7-PLCSIM Advanced

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.