Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0246

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-08-2025

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 SIMATIC, SINEC, SIMAC, RUGGEDCOM, SIMOTION, SINAMICS, SIPROTEC en SINUMERIK.

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)
- Cross-Site Scripting
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- (Remote) code execution (SYSTEM rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot gevoelige gegevens
- Verhogen van rechten

De kwaadwillende heeft hiervoor toegang nodig tot de productieomgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

Siemens heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cert-portal.siemens.com/productcert/html/ssa-094954.html
- https://cert-portal.siemens.com/productcert/html/ssa-177847.html
- https://cert-portal.siemens.com/productcert/html/ssa-186293.html
- https://cert-portal.siemens.com/productcert/html/ssa-282044.html
- https://cert-portal.siemens.com/productcert/html/ssa-493396.html
- https://cert-portal.siemens.com/productcert/html/ssa-493787.html
- https://cert-portal.siemens.com/productcert/html/ssa-517338.html
- https://cert-portal.siemens.com/productcert/html/ssa-529291.html
- https://cert-portal.siemens.com/productcert/html/ssa-665108.html
- https://cert-portal.siemens.com/productcert/html/ssa-674084.html
- https://cert-portal.siemens.com/productcert/html/ssa-707630.html
- https://cert-portal.siemens.com/productcert/html/ssa-894058.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0395	7.5 HIGH
CVE-2025-0665	5.1 MEDIUM
CVE-2025-0725	6.9 MEDIUM
CVE-2025-1390	4.8 MEDIUM
CVE-2025-3277	6.9 MEDIUM
CVE-2025-3360	4.8 MEDIUM
CVE-2025-6395	6.5 MEDIUM
CVE-2025-21694	6.9 MEDIUM
CVE-2025-29087	5.3 MEDIUM
CVE-2025-29088	5.1 MEDIUM
CVE-2025-30033	8.5 HIGH
CVE-2025-30034	6.9 MEDIUM
CVE-2025-32728	4.8 MEDIUM
CVE-2025-32988	6.3 MEDIUM
CVE-2025-32989	6.9 MEDIUM
CVE-2025-32990	6.9 MEDIUM
CVE-2025-33023	5.1 MEDIUM
CVE-2025-40570	2.4 LOW
CVE-2025-40584	6.8 MEDIUM
CVE-2025-40743	8.7 HIGH
CVE-2025-40746	9.4 CRITICAL

CVE-2025-40751	4.8 MEDIUM
CVE-2025-40752	6.8 MEDIUM
CVE-2025-40753	6.8 MEDIUM
CVE-2025-40759	8.5 HIGH
CVE-2025-40761	8.6 HIGH
CVE-2025-40762	7.3 HIGH
CVE-2025-40764	7.3 HIGH
CVE-2025-40766	6.8 MEDIUM
CVE-2025-40767	8.8 HIGH
CVE-2025-40768	7.0 HIGH
CVE-2025-40769	7.5 HIGH
CVE-2025-40770	7.5 HIGH
CVE-2025-47809	8.2 HIGH

CWE's

CWE	Beschrijving
CWE-295	Improper Certificate Validation
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
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-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-20	Improper Input Validation
CWE-1341	Multiple Releases of Same Resource or Handle
CWE-1164	Irrelevant Code
CWE-272	Least Privilege Violation
CWE-131	Incorrect Calculation of Buffer Size
CWE-522	Insufficiently Protected Credentials
CWE-667	Improper Locking
CWE-440	Expected Behavior Violation
CWE-415	Double Free
CWE-617	Reachable Assertion
CWE-427	Uncontrolled Search Path Element
CWE-680	Integer Overflow to Buffer Overflow
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-300	Channel Accessible by Non-Endpoint
CWE-312	Cleartext Storage of Sensitive Information
CWE-190	Integer Overflow or Wraparound
CWE-250	Execution with Unnecessary Privileges
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-476	NULL Pointer Dereference

Getroffen producten

Siemens
RUGGEDCOM ROX MX5000
RUGGEDCOM ROX MX5000RE
RUGGEDCOM ROX RX1400
RUGGEDCOM ROX RX1500
RUGGEDCOM ROX RX1501
RUGGEDCOM ROX RX1510
RUGGEDCOM ROX RX1511
RUGGEDCOM ROX RX1512
RUGGEDCOM ROX RX1524
RUGGEDCOM ROX RX1536
RUGGEDCOM ROX RX5000
SIMATIC Automation Tool
SIMATIC Automation Tool SDK Windows
SIMATIC BATCH V10.0

SIMATIC BATCH V9.1
SIMATIC Control Function Library (CFL) V1.0.0
SIMATIC Control Function Library (CFL) V2.0
SIMATIC Control Function Library (CFL) V3.0
SIMATIC Control Function Library (CFL) V4.0
SIMATIC Energy Suite V17
SIMATIC Energy Suite V18
SIMATIC Energy Suite V19
SIMATIC Logon V1.6
SIMATIC Logon V2.0
SIMATIC MTP CREATOR V3.x
SIMATIC MTP CREATOR V4.x
SIMATIC MTP CREATOR V2.x
SIMATIC MTP CREATOR V5.x
SIMATIC MTP Integrator V1.x
SIMATIC MTP Integrator V2.x

SIMATIC Management Agent
SIMATIC Management Console
SIMATIC NET PC Software V16
SIMATIC NET PC Software V17
SIMATIC NET PC Software V18
SIMATIC NET PC Software V19
SINEC NMS
SINEC Traffic Analyzer
SIMOTION SCOUT TIA V5.4
SIMOTION SCOUT TIA V5.5
SIMOTION SCOUT TIA V5.6
SIMOTION SCOUT TIA V5.7
SIMOTION SCOUT V5.4
SIMOTION SCOUT V5.5
SIMOTION SCOUT V5.6
SIMOTION SCOUT V5.7

SIPROTEC 5 6MD84 (CP300)
SIPROTEC 5 6MD85 (CP300)
SIPROTEC 5 6MD86 (CP300)
SIPROTEC 5 6MD89 (CP300)
SIPROTEC 5 6MU85 (CP300)
SIPROTEC 5 7KE85 (CP300)
SIPROTEC 5 7SA82 (CP150)
SIPROTEC 5 7SA86 (CP300)
SIPROTEC 5 7SA87 (CP300)
SIPROTEC 5 7SD82 (CP150)
SIPROTEC 5 7SD86 (CP300)
SIPROTEC 5 7SD87 (CP300)
SIPROTEC 5 7SJ81 (CP150)
SIPROTEC 5 7SJ82 (CP150)
SIPROTEC 5 7SJ85 (CP300)
SIPROTEC 5 7SJ86 (CP300)

SIPROTEC 5 7SK82 (CP150)
SIPROTEC 5 7SK85 (CP300)
SIPROTEC 5 7SL82 (CP150)
SIPROTEC 5 7SL86 (CP300)
SIPROTEC 5 7SL87 (CP300)
SIPROTEC 5 7SS85 (CP300)
SIPROTEC 5 7ST85 (CP300)
SIPROTEC 5 7ST86 (CP300)
SIPROTEC 5 7SX82 (CP150)
SIPROTEC 5 7SX85 (CP300)
SIPROTEC 5 7SY82 (CP150)
SIPROTEC 5 7UM85 (CP300)
SIPROTEC 5 7UT82 (CP150)
SIPROTEC 5 7UT85 (CP300)
SIPROTEC 5 7UT86 (CP300)
SIPROTEC 5 7UT87 (CP300)

SIPROTEC 5 7VE85 (CP300)
SIPROTEC 5 7VK87 (CP300)
SIPROTEC 5 7VU85 (CP300)
SIPROTEC 5 Compact 7SX800 (CP050)
SINUMERIK 828D PPU.4
SINUMERIK 828D PPU.5
SINUMERIK 840D sl
SINUMERIK MC
SINUMERIK MC V1.15
SINUMERIK ONE
SINUMERIK ONE V6.15

Disclaimer