Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0346

Kwetsbaarheden verholpen in Siemens producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026
Revisie: 1.0.1

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

Update Revisie 1

Inschaling stond abusievelijk op Medium/Medium, is aangepast naar Medium/High.

Feiten

Siemens heeft kwetsbaarheden verholpen in diverse producten als Desigo, Reyrolle, SIMATIC, SCALANCE, SINAMICS en Siveillance.

Duiding

De kwetsbaarheden stellen een kwaadwillende 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)
- (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

De betrokken leveranciers hebben updates uitgebracht om de genoemde kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cert-portal.siemens.com/productcert/html/ssa-019113.html
- https://cert-portal.siemens.com/productcert/html/ssa-142885.html
- https://cert-portal.siemens.com/productcert/html/ssa-157465.html
- https://cert-portal.siemens.com/productcert/html/ssa-216014.html
- https://cert-portal.siemens.com/productcert/html/ssa-229470.html
- https://cert-portal.siemens.com/productcert/html/ssa-254516.html
- https://cert-portal.siemens.com/productcert/html/ssa-282044.html
- https://cert-portal.siemens.com/productcert/html/ssa-327438.html

- https://cert-portal.siemens.com/productcert/html/ssa-328642.html
- https://cert-portal.siemens.com/productcert/html/ssa-330084.html
- https://cert-portal.siemens.com/productcert/html/ssa-331739.html
- https://cert-portal.siemens.com/productcert/html/ssa-434797.html
- https://cert-portal.siemens.com/productcert/html/ssa-503852.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-42384	7.5 HIGH
CVE-2024-42385	4.0 MEDIUM
CVE-2024-42386	8.2 HIGH
CVE-2024-42391	4.3 MEDIUM
CVE-2024-42392	4.0 MEDIUM
CVE-2024-56181	8.4 HIGH
CVE-2024-56182	8.4 HIGH
CVE-2025-15467	9.8 CRITICAL
CVE-2025-30033	8.5 HIGH
CVE-2025-40572	6.8 MEDIUM
CVE-2025-40573	6.7 MEDIUM
CVE-2025-40574	8.5 HIGH
CVE-2025-40575	5.3 MEDIUM
CVE-2025-40576	5.3 MEDIUM
CVE-2025-40577	5.3 MEDIUM
CVE-2025-40578	5.3 MEDIUM
CVE-2025-40579	5.4 MEDIUM

CVE-2025-40580	5.4 MEDIUM
CVE-2025-40581	8.4 HIGH
CVE-2025-40582	8.5 HIGH
CVE-2025-40583	6.7 MEDIUM
CVE-2025-47809	8.2 HIGH
CVE-2026-18963	9.1 CRITICAL
CVE-2026-31431	7.8 HIGH
CVE-2026-34223	8.6 HIGH
CVE-2026-50093	8.9 HIGH
CVE-2026-54798	7.1 HIGH
CVE-2026-54799	8.4 HIGH
CVE-2026-54800	6.3 MEDIUM
CVE-2026-54801	8.6 HIGH
CVE-2026-58113	8.5 HIGH
CVE-2026-62645	9.3 CRITICAL
CVE-2026-62646	9.1 CRITICAL
CVE-2026-62647	9.3 CRITICAL
CVE-2026-62648	8.7 HIGH
CVE-2026-62649	8.7 HIGH
CVE-2026-62650	8.7 HIGH
CVE-2026-62652	6.9 MEDIUM
CVE-2026-62653	7.0 HIGH
CVE-2026-62654	7.0 HIGH

CVE-2026-67367	**9.2 CRITICAL**

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-35	Path Traversal: '.../...//'
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-94	Improper Control of Generation of Code ('Code Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-140	Improper Neutralization of Delimiters
CWE-190	Integer Overflow or Wraparound
CWE-215	Insertion of Sensitive Information Into Debugging Code
CWE-272	Least Privilege Violation
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-306	Missing Authentication for Critical Function
CWE-319	Cleartext Transmission of Sensitive Information
CWE-331	Insufficient Entropy
CWE-427	Uncontrolled Search Path Element
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-457	Use of Uninitialized Variable

CWE-476	NULL Pointer Dereference
CWE-489	Active Debug Code
CWE-494	Download of Code Without Integrity Check
CWE-620	Unverified Password Change
CWE-640	Weak Password Recovery Mechanism for Forgotten Password
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-823	Use of Out-of-range Pointer Offset
CWE-1188	Initialization of a Resource with an Insecure Default
CWE-1288	Improper Validation of Consistency within Input

Getroffen producten

Siemens
CPCI85 Central Processing/ Communication
Desigo CC ClickOnce Client V6
Desigo CC ClickOnce Client V7
Desigo CC Flex Client V6
Desigo CC Flex Client V7
Desigo CC Installed Client V6

Desigo CC Installed Client V7
Desigo CC family V5.0
Desigo CC family V5.1
Desigo CC family V6
Desigo CC family V7
Desigo CC family V8
Desigo CC family V9
Industrial Edge Management
Reyrolle 7SR5
SCALANCE LPE9403
SIMATIC AX Runtime Core Linux Common Debian
SIMATIC AX Runtime Core Linux Common Debian arm64
SIMATIC AX Runtime Core Linux Platform Container Common Debian Development
SIMATIC AX Runtime Core Linux VMWare Development
SIMATIC CN 4100
SIMATIC Field PG M5

SIMATIC Field PG M6
SIMATIC HMI Basic Panels
SIMATIC HMI Comfort Panels
SIMATIC IPC Industrial Edge Device OS (IED-OS)
SIMATIC PDM Maintenance Station V5.0
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP
SIMATIC WinCC
SIMATIC eaSie Core Package
Simatic IOT2050 Firmware
Siplant
Siveillance Control Pro V3.0
Siveillance Control Pro V4.0
Siveillance Control V3.0
Siveillance Control V4.0
Teamcenter V2412
Teamcenter V2506

Teamcenter V2512
Teamcenter V2606
sicore_base_system
simove Fleet Manager

Disclaimer