Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0051

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-02-2026

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 Desigo, NX, Polarion, SENTRON, Simcenter, SINEC, SIPORT, Siveillance, 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
- (Remote) code execution (root/admin rechten)
- Toegang tot systeemgegevens
- Verhogen van rechten

Van de SIPORT Desktop Client Application meldt Siemens dat deze verouderd is en niet voorzien van moderne beveiligingsmaatregelen. Siemens geeft aan deze ook niet meer in te bouwen en het onderhoud op de Desktop Client te stoppen. Siemens adviseert om over te schakelen naar de modernere web-management-omgeving. Wel heeft Siemens mitigerende maatregelen gepubliceerd in een Security Bulletin, om het risico zoveel als mogelijk te beperken tot de migratie is afgerond en de vaste Desktop Clients zijn uitgefaseerd.

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-035571.html
- https://cert-portal.siemens.com/productcert/html/ssa-311973.html
- https://cert-portal.siemens.com/productcert/html/ssa-445819.html
- https://cert-portal.siemens.com/productcert/html/ssa-507364.html
- https://cert-portal.siemens.com/productcert/html/ssa-535115.html
- https://cert-portal.siemens.com/productcert/html/ssa-625934.html
- https://cert-portal.siemens.com/productcert/html/ssa-965753.html

› https://cert-portal.siemens.com/productcert/html/ssb-491780.html

Kwetsbaarheden

CVE	CVSS Score
› CVE-2023-38545	9.8 CRITICAL
› CVE-2025-0836	5.3 MEDIUM
› CVE-2025-40587	6.2 MEDIUM
› CVE-2025-40936	7.7 HIGH
› CVE-2026-22923	8.5 HIGH
› CVE-2026-23715	8.5 HIGH
› CVE-2026-23716	8.5 HIGH
› CVE-2026-23717	8.5 HIGH
› CVE-2026-23718	8.5 HIGH
› CVE-2026-23719	8.5 HIGH
› CVE-2026-23720	8.5 HIGH
› CVE-2026-25655	8.5 HIGH
› CVE-2026-25656	8.5 HIGH

CWE's

CWE	Beschrijving
› CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
› CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
› CWE-121	Stack-based Buffer Overflow
› CWE-122	Heap-based Buffer Overflow

CWE-125	Out-of-bounds Read
CWE-427	Uncontrolled Search Path Element
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization

Getroffen producten

Siemens
Cpu 1518F-4 Pn/Dp Mfp Firmware
Desigo CC family V6
Desigo CC family V7
Desigo CC family V8
Desigo CC family V9
NX
PS/IGES Parasolid Translator Component
Polarion V2404
Polarion V2410
RUGGEDCOM APE1808
SENTRON Powermanager V6
SENTRON Powermanager V7

SENTRON Powermanager V8
SENTRON Powermanager V9
SIMATIC RTLS Locating Manager
SIMATIC RTLS Locating Manager (6GT2780-0DA00)
SIMATIC RTLS Locating Manager (6GT2780-0DA10)
SIMATIC RTLS Locating Manager (6GT2780-0DA20)
SIMATIC RTLS Locating Manager (6GT2780-0DA30)
SIMATIC RTLS Locating Manager (6GT2780-1EA10)
SIMATIC RTLS Locating Manager (6GT2780-1EA20)
SIMATIC RTLS Locating Manager (6GT2780-1EA30)
SIMATIC S7
SIMATIC S7-1500
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)

SINEC NMS
SINEC Network Management System
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0)
Simcenter Femap
Simcenter Nastran
Siveillance Video V2022 R3
Siveillance Video V2023 R1
Siveillance Video V2023 R2
Siveillance Video V2023 R3
Siveillance Video V2024 R1
Siveillance Video V2025
Solid Edge
User Management Component (UMC)

Disclaimer