Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0282

Kwetsbaarheden verholpen in Siemens producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-08-2026

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, Parasolid, RUGGEDCOM, SIMATIC, Siveillance en 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)
- (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 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-069220.html
- https://cert-portal.siemens.com/productcert/html/ssa-077553.html
- https://cert-portal.siemens.com/productcert/html/ssa-127084.html
- https://cert-portal.siemens.com/productcert/html/ssa-138516.html
- https://cert-portal.siemens.com/productcert/html/ssa-584312.html
- https://cert-portal.siemens.com/productcert/html/ssa-621657.html
- https://cert-portal.siemens.com/productcert/html/ssa-751328.html
- https://cert-portal.siemens.com/productcert/html/ssa-781903.html
- https://cert-portal.siemens.com/productcert/html/ssa-825228.html
- https://cert-portal.siemens.com/productcert/html/ssa-834709.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-3014	6.4 MEDIUM
CVE-2026-23573	6.1 MEDIUM
CVE-2026-50058	7.3 HIGH
CVE-2026-50059	7.8 HIGH
CVE-2026-50060	7.8 HIGH
CVE-2026-50061	7.8 HIGH
CVE-2026-50062	7.8 HIGH
CVE-2026-50063	7.8 HIGH
CVE-2026-50064	7.3 HIGH
CVE-2026-57262	7.0 HIGH
CVE-2026-57263	6.8 MEDIUM
CVE-2026-58115	10.0 CRITICAL
CVE-2026-59086	7.8 HIGH
CVE-2026-59693	4.3 MEDIUM
CVE-2026-59700	7.8 HIGH
CVE-2026-59701	7.8 HIGH
CVE-2026-59839	5.5 MEDIUM
CVE-2026-64629	7.8 HIGH
CVE-2026-69108	6.0 MEDIUM
CVE-2026-69109	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('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-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-275	Permission Issues
CWE-306	Missing Authentication for Critical Function
CWE-321	Use of Hard-coded Cryptographic Key
CWE-416	Use After Free
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-759	Use of a One-Way Hash without a Salt
CWE-787	Out-of-bounds Write

Getroffen producten

Siemens
Desigo DXR2
Desigo PXC3

Desigo PXC4
Desigo PXC5.E003
Desigo PXC5.E24
Desigo PXC7
LOGO! Soft Comfort
Parasolid V38.0
Parasolid V38.1
RUGGEDCOM APE1808
SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2)
Siemens License Server (SLS)
Simcenter Femap
Simcenter Nastran
Siveillance Video V2023 R3
Siveillance Video V2024 R1
Siveillance Video V2025
Solid Edge SE2025

Solid Edge
SE2026

Disclaimer