Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0211

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-07-2025

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, SIPROTEC, Solid Edge en TIA,

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)
- SQL Injection
- 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/pdf/ssa-460466.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-573669.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-626991.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-904646.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-078892.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-091753.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-23364	6.9 MEDIUM
CVE-2025-23365	8.5 HIGH
CVE-2025-27127	5.3 MEDIUM
CVE-2025-40593	7.1 HIGH
CVE-2025-40735	8.7 HIGH
CVE-2025-40736	9.3 CRITICAL
CVE-2025-40737	8.7 HIGH
CVE-2025-40738	8.7 HIGH
CVE-2025-40739	7.3 HIGH
CVE-2025-40740	7.3 HIGH
CVE-2025-40741	7.3 HIGH
CVE-2025-40742	6.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-598	Use of GET Request Method With Sensitive Query Strings
CWE-347	Improper Verification of Cryptographic Signature
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-125	Out-of-bounds Read
CWE-306	Missing Authentication for Critical Function
CWE-284	Improper Access Control

CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-121	Stack-based Buffer Overflow
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-20	Improper Input Validation

Disclaimer