Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0008

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-01-2025

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 Industrial Edge Management, Mendix, SIMATIC, SIPROTEC en Siveillance.

Duiding

De kwetsbaarheden stellen een kwaadwillende mogelijk in staat aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site-Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- Omzeilen van authenticatie
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens

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.

Dreigingsinformatie

CVE's toe te voegen:

CVE-2024-12569, CVE-2024-45385, CVE-2024-47100, CVE-2024-53649, CVE-2024-56841

Referenties

- https://cert-portal.siemens.com/productcert/pdf/ssa-194557.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-314390.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-404759.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-416411.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-717113.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-12569	
CVE-2024-45385	4.7 MEDIUM
CVE-2024-47100	7.1 HIGH
CVE-2024-53649	6.5 MEDIUM
CVE-2024-56841	7.4 HIGH

CWE's

CWE	Beschrijving
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')
CWE-532	Insertion of Sensitive Information into Log File
CWE-552	Files or Directories Accessible to External Parties
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

siemens
simatic_s7-1200_cpu_1215fc_dc_dc_rly
simatic_s7-1200_cpu_1217c_dc_dc_dc
siplus_s7-1200_cpu_1212_ac_dc_rly
siplus_s7-1200_cpu_1212_dc_dc_rly
siplus_s7-1200_cpu_1212c_dc_dc_dc

siplus_s7-1200_cpu_1212c_dc_dc_dc_rail
siplus_s7-1200_cpu_1214_ac_dc_rly
siplus_s7-1200_cpu_1214_dc_dc_dc
siplus_s7-1200_cpu_1214_dc_dc_rly
siplus_s7-1200_cpu_1214c_dc_dc_dc_rail
siplus_s7-1200_cpu_1214fc_dc_dc_dc
siplus_s7-1200_cpu_1214fc_dc_dc_rly
siplus_s7-1200_cpu_1215_ac_dc_rly
siplus_s7-1200_cpu_1215_dc_dc_dc
siplus_s7-1200_cpu_1215_dc_dc_rly
siplus_s7-1200_cpu_1215c_dc_dc_dc
siplus_s7-1200_cpu_1215fc_dc_dc_dc
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__cp100_
siprotec_5_7sa82__cp150_
siprotec_5_7sa86__cp300_
siprotec_5_7sa87__cp300_
siprotec_5_7sd82__cp100_
siprotec_5_7sd82__cp150_
siprotec_5_7sd86__cp300_
siprotec_5_7sd87__cp300_

siprotec_5_7sj81__cp100_
siprotec_5_7sj81__cp150_
siprotec_5_7sj82__cp100_
siprotec_5_7sj82__cp150_
siprotec_5_7sj85__cp300_
siprotec_5_7sj86__cp300_
siprotec_5_7sk82__cp100_
siprotec_5_7sk82__cp150_
siprotec_5_7sk85__cp300_
siprotec_5_7sl82__cp100_
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_
industrial_edge_management_os__iem-os_
mendix_ldap
simatic_s7-1200_cpu_1211c_ac_dc_rly
simatic_s7-1200_cpu_1211c_dc_dc_dc
simatic_s7-1200_cpu_1211c_dc_dc_rly

simatic_s7-1200_cpu_1212c_ac_dc_rly
simatic_s7-1200_cpu_1212c_dc_dc_dc
simatic_s7-1200_cpu_1212c_dc_dc_rly
simatic_s7-1200_cpu_1212fc_dc_dc_dc
simatic_s7-1200_cpu_1212fc_dc_dc_rly
simatic_s7-1200_cpu_1214c_ac_dc_rly
simatic_s7-1200_cpu_1214c_dc_dc_dc
simatic_s7-1200_cpu_1214c_dc_dc_rly
simatic_s7-1200_cpu_1214fc_dc_dc_dc
simatic_s7-1200_cpu_1214fc_dc_dc_rly
simatic_s7-1200_cpu_1215c_ac_dc_rly
simatic_s7-1200_cpu_1215c_dc_dc_dc
simatic_s7-1200_cpu_1215c_dc_dc_rly
simatic_s7-1200_cpu_1215fc_dc_dc_dc
siprotec_5_7ut82__cp100_
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_

Disclaimer