Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0282

Kwetsbaarheden verholpen in Siemens Producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-07-2024

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 Mendix, RUGGEDOM, SIMATIC, SINEMA, SIPROTEC en de Engineering Platforms voor diverse systemen.

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
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens
- Verhoogde gebruikersrechten

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-064222.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-088132.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-170375.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-313039.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-364175.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-381581.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-698820.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-722010.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-723487.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-750499.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-779936.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-824889.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-868282.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-883918.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-928781.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-998949.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-32260	
CVE-2023-7066	
CVE-2023-27321	
CVE-2023-32735	
CVE-2023-32737	
CVE-2023-46720	
CVE-2023-48795	
CVE-2023-52237	7.5 HIGH
CVE-2023-52238	
CVE-2023-52891	
CVE-2024-21754	
CVE-2024-23111	
CVE-2024-26010	
CVE-2024-30321	
CVE-2024-32055	7.8 HIGH
CVE-2024-32056	
CVE-2024-32057	7.8 HIGH
CVE-2024-32058	7.8 HIGH

CVE-2024-32059	7.8 HIGH
CVE-2024-32060	7.8 HIGH
CVE-2024-32061	7.8 HIGH
CVE-2024-32062	7.8 HIGH
CVE-2024-32063	7.8 HIGH
CVE-2024-32064	7.8 HIGH
CVE-2024-32065	7.8 HIGH
CVE-2024-32066	7.8 HIGH
CVE-2024-33577	
CVE-2024-33653	
CVE-2024-33654	
CVE-2024-37996	3.3 LOW
CVE-2024-37997	7.8 HIGH
CVE-2024-38278	
CVE-2024-38867	
CVE-2024-39567	
CVE-2024-39568	
CVE-2024-39569	
CVE-2024-39570	
CVE-2024-39571	
CVE-2024-39675	
CVE-2024-39865	
CVE-2024-39866	

CVE-2024-39867	
CVE-2024-39868	
CVE-2024-39869	
CVE-2024-39870	
CVE-2024-39871	
CVE-2024-39872	
CVE-2024-39873	
CVE-2024-39874	
CVE-2024-39875	
CVE-2024-39876	
CVE-2024-39888	7.5 HIGH
CVE-2024-3596	

CWE's

CWE	Beschrijving
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-1325	Improperly Controlled Sequential Memory Allocation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-222	Truncation of Security-relevant Information
CWE-266	Incorrect Privilege Assignment
CWE-267	Privilege Defined With Unsafe Actions
CWE-286	Incorrect User Management

CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-326	Inadequate Encryption Strength
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-378	Creation of Temporary File With Insecure Permissions
CWE-400	Uncontrolled Resource Consumption
CWE-425	Direct Request ('Forced Browsing')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-476	NULL Pointer Dereference
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-502	Deserialization of Untrusted Data
CWE-547	Use of Hard-coded, Security-relevant Constants
CWE-602	Client-Side Enforcement of Server-Side Security
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-863	Incorrect Authorization
CWE-916	Use of Password Hash With Insufficient Computational Effort
CWE-924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel

Getroffen producten

siemens
jt_open
mendix_encryption
plm_xml_sdk
ps_iges_parasolid_translator_component
ruggedcom_i800
ruggedcom_i800nc
ruggedcom

Disclaimer