



NCSC-2024-0332

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2024

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 COMOS, INTRALOG, LOGO!, NX, SCALANCE, SINEC en Teamcenter.

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 (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Spoofing
- 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-087301.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-357412.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-417547.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-659443.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-716317.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-720392.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-784301.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-856475.pdf>
- <https://cert-portal.siemens.com/productcert/pdf/ssa-921449.pdf>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2023-4611	
> CVE-2023-5180	
> CVE-2023-5868	
> CVE-2023-5869	
> CVE-2023-5870	
> CVE-2023-6378	
> CVE-2023-6481	
> CVE-2023-26495	
> CVE-2023-31122	
> CVE-2023-34050	
> CVE-2023-39615	
> CVE-2023-42794	
> CVE-2023-42795	
> CVE-2023-43622	
> CVE-2023-44321	
> CVE-2023-44487	
> CVE-2023-45648	
> CVE-2023-45802	
> CVE-2023-46120	
> CVE-2023-46280	
> CVE-2023-46589	

> CVE-2023-52425
> CVE-2023-52426
> CVE-2024-0056
> CVE-2024-0985
> CVE-2024-25062
> CVE-2024-28182
> CVE-2024-28757
> CVE-2024-30045
> CVE-2024-32635
> CVE-2024-32636
> CVE-2024-32637
> CVE-2024-36398
> CVE-2024-39922
> CVE-2024-41681
> CVE-2024-41682
> CVE-2024-41683
> CVE-2024-41903
> CVE-2024-41904
> CVE-2024-41905
> CVE-2024-41906
> CVE-2024-41907
> CVE-2024-41908
> CVE-2024-41938

➤ CVE-2024-41939
➤ CVE-2024-41940
➤ CVE-2024-41941
➤ CVE-2024-41976
➤ CVE-2024-41977
➤ CVE-2024-41978

CWE's

CWE	Beschrijving
➤ CWE-125	Out-of-bounds Read
➤ CWE-20	Improper Input Validation
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-250	Execution with Unnecessary Privileges
➤ CWE-256	Plaintext Storage of a Password
➤ CWE-269	Improper Privilege Management
➤ CWE-284	Improper Access Control
➤ CWE-307	Improper Restriction of Excessive Authentication Attempts
➤ CWE-326	Inadequate Encryption Strength
➤ CWE-358	Improperly Implemented Security Check for Standard
➤ CWE-488	Exposure of Data Element to Wrong Session
➤ CWE-521	Weak Password Requirements
➤ CWE-524	Use of Cache Containing Sensitive Information
➤ CWE-532	Insertion of Sensitive Information into Log File
➤ CWE-863	Incorrect Authorization

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.