Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0225

Kwetsbaarheden verholpen in Siemens SICORE

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-07-2026

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 SICORE Base systemen, specifiek in versies onder V26.20.

Duiding

De kwetsbaarheden bevinden zich in meerdere onderdelen van de CPCI85 en SICORE Base systemen. Een kwetsbaarheid maakt het mogelijk voor een geauthenticeerde aanvaller om via een HTTP-toegankelijke debugging interface de webservice te laten crashen, wat leidt tot een denial-of-service. Daarnaast bevat de firmware update procedure een zwakte in de validatie van firmware handtekeningen, waardoor een aanvaller malafide firmware kan installeren en daarmee persistente code-uitvoering kan verkrijgen. Verder is er een configuratiefout waarbij alle OPC UA beveiligingsmechanismen standaard uitgeschakeld zijn, waardoor authenticatie en autorisatie kunnen worden omzeild en onbevoegde toegang tot kritieke systeemfuncties mogelijk is. Tot slot is er een kwetsbaarheid in de web API die onvoldoende validatie van authenticatiegegevens uitvoert bij wijzigingen aan administratieve accounts, wat een geauthenticeerde aanvaller in staat stelt om beveiligingscontroles te omzeilen en privileges te escaleren.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de productie-omgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

Siemens heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cert-portal.siemens.com/productcert/html/ssa-229470.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-54798	7.1 HIGH
CVE-2026-54799	10.0 CRITICAL
CVE-2026-54800	10.0 CRITICAL
CVE-2026-54801	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-285	Improper Authorization
CWE-345	Insufficient Verification of Data Authenticity
CWE-400	Uncontrolled Resource Consumption
CWE-489	Active Debug Code
CWE-620	Unverified Password Change
CWE-1188	Initialization of a Resource with an Insecure Default

Getroffen producten

Siemens
CPCI85 Central Processing Communication, SICORE Base System
SICORE Base system

Disclaimer