Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0246

Kwetsbaarheden verholpen in Siemens producten

2024-06-11 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Siemens heeft kwetsbaarheden verholpen in diverse producten, zoals SCALANCE, SICAM, Tecnomatix, SITOP en PowerSys.

Interpretaties

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 beveiligingsmaatregel
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- 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-024584.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-196737.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-238730.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-319319.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-337522.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-341067.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-481506.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-540640.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-620338.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-625862.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-690517.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-879734.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-900277.pdf