Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2024-0452

## Kwetsbaarheden verholpen in Siemens Tecnomatix Plant Simulation

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-11-2024

**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 Tecnomatix Plant Simulation.

## Duiding

De kwetsbaarheden bevinden zich in de wijze waarop Tecnomatix Plant Simulation speciaal vervaardigde WRL-bestanden verwerkt. Deze kwetsbaarheden omvatten onder andere out-of-bounds writes, use-after-free en stack-based overflows, die allemaal kunnen worden misbruikt door kwaadwillenden om willekeurige code uit te voeren binnen de context van het huidige proces. Dit kan leiden tot ongeautoriseerde toegang en controle over de getroffen applicaties, wat een ernstige bedreiging vormt voor de integriteit en beveiliging van de systemen.

Voor succesvol misbruik moet de kwaadwillende toegang hebben 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/html/ssa-824503.html

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2024-52565 | 7.8 HIGH |
| CVE-2024-52566 | 7.8 HIGH |
| CVE-2024-52567 | 7.8 HIGH |
| CVE-2024-52568 | 7.8 HIGH |
| CVE-2024-52569 | 7.8 HIGH |
| CVE-2024-52570 | 7.8 HIGH |

| | |
|---|---|
| CVE-2024-52571 | 7.8 HIGH |
| CVE-2024-52572 | 7.8 HIGH |
| CVE-2024-52573 | 7.8 HIGH |
| CVE-2024-52574 | 7.8 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-125 | Out-of-bounds Read |
| CWE-416 | Use After Free |
| CWE-787 | Out-of-bounds Write |
| CWE-121 | Stack-based Buffer Overflow |

## Getroffen producten

| **siemens** |
|---|
| tecnomatix_plant_simulation |
| tecnomatix_plant_simulation_v2302 |
| tecnomatix_plant_simulation_v2404 |

## Disclaimer