



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
➤ <a href="#">CVE-2024-52565</a>	7.8 HIGH
➤ <a href="#">CVE-2024-52566</a>	7.8 HIGH
➤ <a href="#">CVE-2024-52567</a>	7.8 HIGH
➤ <a href="#">CVE-2024-52568</a>	7.8 HIGH
➤ <a href="#">CVE-2024-52569</a>	7.8 HIGH
➤ <a href="#">CVE-2024-52570</a>	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
> CVE-125	Out-of-bounds Read
> CVE-416	Use After Free
> CVE-787	Out-of-bounds Write
> CVE-121	Stack-based Buffer Overflow

## Getroffen producten

<b>siemens</b>
tecnomatix_plant_simulation
tecnomatix_plant_simulation_v2302
tecnomatix_plant_simulation_v2404

## 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.