Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0345

## Kwetsbaarheden verholpen in Rockwell Automation FactoryTalk

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 31-10-2025

**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

Rockwell Automation heeft kwetsbaarheden verholpen in FactoryTalk View Machine Edition.

## Duiding

De kwetsbaarheden omvatten een authenticatie-bypass die ongeautoriseerde toegang tot het bestandssysteem en diagnostische informatie van de PanelView Plus 7 Series B toestaat. Daarnaast is er een pad-traversal kwetsbaarheid die ongeauthenticeerde aanvallers in staat stelt om bestanden binnen het besturingssysteem van het apparaat te verwijderen. Verder is er een XML External Entity (XXE) kwetsbaarheid die kan leiden tot tijdelijke denial-of-service. Ook zijn er kwetsbaarheden in de Microsoft Installer File (MSI) die door geauthenticeerde aanvallers kunnen worden misbruikt om SYSTEM-niveau toegang te verkrijgen. Deze kwetsbaarheden kunnen leiden tot ernstige gevolgen, waaronder dataverlies, systeeminstabiliteit en ongeautoriseerde controle over systeembronnen.

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

## Oplossingen

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

## Referenties

- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1752.html
- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1753.html
- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1754.html

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2025-9063 | 7.0 HIGH |
| CVE-2025-9064 | 8.7 HIGH |
| CVE-2025-9066 | 8.7 HIGH |

| | |
|---|---|
| CVE-2025-9067 | 8.5 HIGH |
| CVE-2025-9068 | 8.5 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-20 | Improper Input Validation |
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CWE-269 | Improper Privilege Management |
| CWE-287 | Improper Authentication |
| CWE-404 | Improper Resource Shutdown or Release |

## Getroffen producten

| **Rockwell Automation** |
|---|
| FactoryTalk |
| FactoryTalk Linx |
| FactoryTalk View Machine Edition |
| FactoryTalk ViewPoint |
| PanelView Plus 7 Performance B |

## Disclaimer