Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0056

## Kwetsbaarheden verholpen in Schneider Electric ASCO

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-02-2025

**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

Schneider Electric heeft kwetsbaarheden verholpen in ASCO Annunciator

## Duiding

De kwetsbaarheden omvatten een kritieke kwetsbaarheid die het mogelijk maakt om kwaadaardige firmware te downloaden zonder integriteitscontroles, wat kan leiden tot onbruikbaarheid van het apparaat. Daarnaast is er een kwetsbaarheid die voortkomt uit het toewijzen van middelen zonder passende limieten, wat de functionaliteit van webservers ernstig kan beïnvloeden. Een andere kwetsbaarheid betreft de overdracht van gevoelige informatie in platte tekst, wat kan resulteren in gegevensblootstelling bij onderschepping van netwerkverkeer. Tot slot is er een kwetsbaarheid die onbeperkte upload van gevaarlijke bestandstypen mogelijk maakt, wat kan leiden tot compromittering van systeemintegriteit en operationele storingen.

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

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

## Referenties

› https://download.schneider-electric.com/files?p_Doc_Ref=sevd-2025-042-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-042-01.pdf

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| › CVE-2025-1058 | 7.2 HIGH |
| › CVE-2025-1059 | 8.7 HIGH |
| › CVE-2025-1060 | 8.7 HIGH |
| › CVE-2025-1070 | 7.2 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-494 | Download of Code Without Integrity Check |
| CWE-319 | Cleartext Transmission of Sensitive Information |
| CWE-434 | Unrestricted Upload of File with Dangerous Type |
| CWE-770 | Allocation of Resources Without Limits or Throttling |

## Getroffen producten

| **schneider_electric** |
|---|
| asco_5310_single-channel_remote_annunciator |
| asco_5350_eight_channel_remote_annunciator |

## Disclaimer