



## Advisory NCSC-2024-0244

# Kwetsbaarheden verholpen in Schneider Electric Sage RTU systemen

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.first.org/tlp](http://www.first.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](mailto:info@ncsc.nl)

## Feiten

Schneider Electric heeft kwetsbaarheden verholpen in Sage RTU apparatuur.

---

## Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van authenticatie
- Omzeilen van beveiligingsmaatregel
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens

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

---

## Oplossingen

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

---

## Referenties

- [https://download.schneider-electric.com/files?p\\_Doc\\_Ref=SEVD-2024-163-05&p\\_enDocType=Security+and+Safety+Notice&p\\_File](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-163-05&p_enDocType=Security+and+Safety+Notice&p_File)
- [https://download.schneider-electric.com/files?p\\_Doc\\_Ref=SEVD-2024-163-05&p\\_enDocType=Security+and+Safety+Notice&p\\_File](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-163-05&p_enDocType=Security+and+Safety+Notice&p_File)