

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans SCADA Schneider Electric Modicon**

### Gestion du document

Référence	CERTFR-2017-AVI-100
Titre	Multiples vulnérabilités dans SCADA Schneider Electric Modicon
Date de la première version	05 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Schneider Electric SEVD-2017-075-01 du 16 mars 2017 Bulletin de sécurité Schneider Electric SEVD-2017-075-02 du 16 mars 2017 Bulletin de sécurité Schneider Electric SEVD-2017-075-03 du 16 mars 2017
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

### 1 - Risque(s)

- contournement de la politique de sécurité
- atteinte à la confidentialité des données

### 2 - Systèmes affectés

- Micrologiciel de Schneider Electric Modicon M241 versions antérieures à v4.0.5.11
- Micrologiciel de Schneider Electric Modicon M251 versions antérieures à v4.0.5.11
- Micrologiciel de Schneider Electric Modicon M221 versions antérieures à v1.5.0.0

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *SCADA Schneider Electric Modicon*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

### 4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 - Documentation

- Bulletin de sécurité Schneider Electric SEVD-2017-075-01 du 16 mars 2017  
[http://download.schneider-electric.com/files?p\\_enDocType=Technical+leaflet&p\\_File\\_Id=6822753657&p\\_File\\_Name=SEVD-2017-075-01+Modicon+TCP+Predictability.pdf&p\\_Reference=SEVD-2017-075-01](http://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=6822753657&p_File_Name=SEVD-2017-075-01+Modicon+TCP+Predictability.pdf&p_Reference=SEVD-2017-075-01)
- Bulletin de sécurité Schneider Electric SEVD-2017-075-02 du 16 mars 2017  
[http://download.schneider-electric.com/files?p\\_enDocType=Technical+leaflet&p\\_File\\_Id=6822753674&p\\_File\\_Name=SEVD-2017-075-02+Modicon+Authentication+Bypass-Session+Cookie.pdf&p\\_Reference=SEVD-2017-075-02](http://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=6822753674&p_File_Name=SEVD-2017-075-02+Modicon+Authentication+Bypass-Session+Cookie.pdf&p_Reference=SEVD-2017-075-02)
- Bulletin de sécurité Schneider Electric SEVD-2017-075-03 du 16 mars 2017  
[http://download.schneider-electric.com/files?p\\_enDocType=Technical+leaflet&p\\_File\\_Id=6822753691&p\\_File\\_Name=SEVD-2017-075-03+Modicon+Authentication+Bypass-+Credential.pdf&p\\_Reference=SEVD-2017-075-03](http://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=6822753691&p_File_Name=SEVD-2017-075-03+Modicon+Authentication+Bypass-+Credential.pdf&p_Reference=SEVD-2017-075-03)

## Gestion détaillée du document

05 avril 2017 version initiale.

---

Conditions d'utilisation de ce document :	<a href="http://cert.ssi.gouv.fr/cert-fr/apropos.html">http://cert.ssi.gouv.fr/cert-fr/apropos.html</a>
Dernière version de ce document :	<a href="http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-100">http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-100</a>

---