

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans SCADA Schneider homeLYnk Controller

Gestion du document

Référence	CERTFR-2017-AVI-024
Titre	Vulnérabilité dans SCADA Schneider homeLYnk Controller
Date de la première version	20 janvier 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Schneider SEVD-2017-011-01v2 du 18 janvier 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)

- injection de code indirecte à distance

2 - Systèmes affectés

homeLYnk Controller LSS100100 toutes les versions antérieures à V1.5.0

3 - Résumé

Une vulnérabilité a été corrigée dans *SCADA Schneider homeLYnk Controller*. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS).

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 SEVD-2017-011-01v2 du 18 janvier 2017
http://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=5989386180&p_File_Name=SEVD-2017-011-01+HomeLYnk+Controller+v2.pdf&p_Reference=SEVD-2017-011-01

– Référence CVE CVE-2017-5157
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5157>

Gestion détaillée du document

20 janvier 2017 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-024>
