Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 23 février 2017
N° CERTFR-2017-AVI-059

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM NMS

Gestion du document

Référence	CERTFR-2017-AVI-059
Titre	Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM NMS
Date de la première version	23 février 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité SCADA Siemens SSA-363881 du 22 février 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
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

Siemens RUGGEDCOM NMS versions antérieures à V2.1 sur Windows et Linux

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *SCADA Siemens RUGGEDCOM NMS*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une injection de code indirecte à distance (XSS) et une injection de requêtes illégitimes par rebond (CSRF).

4 - Solution

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

5 - Documentation

- Bulletin de sécurité SCADA Siemens SSA-363881 du 22 février 2017
  http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-363881.pdf
- Référence CVE CVE-2017-2682
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2682
- Référence CVE CVE-2017-2683
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2683

Gestion détaillée du document

23 février 2017 version initiale.