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 29 mars 2017
N° CERTFR-2017-ALE-006

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM ROX I

Gestion du document

Référence	CERTFR-2017-ALE-006
Titre	Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM ROX I
Date de la première version	29 mars 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-327980 du 28 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)

- injection de requêtes illégitimes par rebond
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

RUGGEDCOM ROX I toutes versions

3 - Résumé

De multiples vulnérabilités ont été découvertes dans *SCADA Siemens RUGGEDCOM ROX I*. Certaines d'entre elles permettent à un attaquant de provoquer injection de requêtes illégitimes par rebond, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

4 - Contournement provisoire

Plusieurs vulnérabilités ont été reportées dans les équipements Siemens RUGGEDCOM ROX I.
Parmi les vulnérabilités décrites par l'éditeur, la CVE-2017-2688 permet à l'attaquant d'effectuer des actions avec les privilèges d'un utilisateur. L'attaquant doit inciter un utilisateur authentifié à visiter une page malveillante ou à

cliquer sur un lien malveillant. La vulnérabilité CVE-2017-2689 permet quant à elle un accès privilégié au système de fichier et autorise la modification de la configuration. L'exploitation de cette vulnérabilité nécessite un accès authentifié préalable à l'interface web de l'équipement sur le port TCP 10000.

Dans l'attente d'un correctif, l'éditeur à publié des éléments permettant d'atténuer les risques portant sur les systèmes Siemens RUGGEDCOM ROX I.

Se référer au bulletin de l'éditeur pour une liste exhaustive des mesures de prévention à mettre en œuvre (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Siemens SSA-327980 du 28 mars 2017
  http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-327980.pdf
- Référence CVE CVE-2017-2686
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2686
- Référence CVE CVE-2017-2687
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2687
- Référence CVE (CVE-2017-2688
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=(CVE-2017-2688
- Référence CVE CVE-2017-2689
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2689
- Référence CVE CVE-2017-6864
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6864

Gestion détaillée du document

29 mars 2017 version initiale.