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 08 avril 2015
N° CERTFR-2015-AVI-138

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA Siemens SIMATIC

Gestion du document

Référence	CERTFR-2015-AVI-138
Titre	Multiples vulnérabilités dans SCADA Siemens SIMATIC
Date de la première version	08 avril 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-487246 du 08 avril 2015
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)

- déni de service
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- SIMATIC HMI Basic Panels 2nd Generation: toute les versions ayant WinCC (TIA Portal) inférieure à V13 SP1 Upd2
- SIMATIC HMI Comfort Panels: toute les versions ayant WinCC (TIA Portal) inférieure à V13 SP1 Upd2
- SIMATIC WinCC Runtime Advanced: toute les versions ayant WinCC (TIA Portal) inférieure à V13 SP1 Upd2
- SIMATIC WinCC Runtime Professional: toute les versions ayant WinCC (TIA Portal) inférieure à V13 SP1 Upd2
- SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal): toute les versions
- SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal): toute les versions
- SIMATIC HMI Multi Panels (WinCC TIA Portal): toute les versions
- SIMATIC NET PC-Software V12: toute les versions inférieures à V12 SP2 HF3
- SIMATIC NET PC-Software V13: toute les versions inférieures à V13 HF1
- SIMATIC WinCC V7.X: toute les versions inférieures à v7.3 Upd4
- SIMATIC Automation Tool: toute les versions inférieures à v1.0.2

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *SCADA Siemens SIMATIC*. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à l'intégrité des données 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 Siemens SSA-487246 du 08 avril 2015
  http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-487246.pdf
- Référence CVE CVE-2015-1601
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1601
- Référence CVE CVE-2015-2822
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2822

Gestion détaillée du document

08 avril 2015 version initiale.