

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le système SCADA Wind River VxWorks

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-218>

Gestion du document

Référence	CERTA-2013-AVI-218
Titre	Multiples vulnérabilités dans le système SCADA Wind River VxWorks
Date de la première version	04 avril 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wind River ICESA-13-091-01 du 01 avril 2013
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)

- exécution de code arbitraire à distance
- déni de service à distance

2 Systèmes affectés

Produits Wind River utilisant VxWorks version 5.5 à 6.9

3 Résumé

De multiples vulnérabilités ont été corrigées dans le système SCADA *Wind River VxWorks*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité JVN JVNDB-2013-000018 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000018.html>
- Bulletin de sécurité JVN JVNDB-2013-000019 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000019.html>
- Bulletin de sécurité JVN JVNDB-2013-000020 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000020.html>
- Bulletin de sécurité JVN JVNDB-2013-000021 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000021.html>
- Bulletin de sécurité JVN JVNDB-2013-000022 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000022.html>
- Bulletin de sécurité JVN JVNDB-2013-000023 du 01 avril 2013
<http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000023.html>
- Bulletin de sécurité Wind River ICSA-13-091-01 du 01 avril 2013
<http://ics-cert.us-cert.gov/pdf/ICSA-13-091-01.pdf>
- Référence CVE CVE-2013-0711
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0711>
- Référence CVE CVE-2013-0712
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0712>
- Référence CVE CVE-2013-0713
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0713>
- Référence CVE CVE-2013-0714
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0714>
- Référence CVE CVE-2013-0715
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0715>
- Référence CVE CVE-2013-0716
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0716>

Gestion détaillée du document

04 avril 2013 version initiale.