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 10 juillet 2014
N° CERTFR-2014-AVI-308

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Juniper Junos

Gestion du document

Référence	CERTFR-2014-AVI-308
Titre	Multiples vulnérabilités dans Juniper Junos
Date de la première version	10 juillet 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10613 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10633 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10634 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10635 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10637 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10638 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10640 du 09 juillet 2014 Bulletin de sécurité Juniper JSA10641 du 09 juillet 2014
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 à distance
- élévation de privilèges

2 - Systèmes affectés

- Junos (toutes les versions)
- Passerelles de services SRX Series

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Juniper Junos*. Elles permettent à un attaquant de provoquer un déni de service à distance et une élévation de privilèges.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Juniper JSA10613 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10613&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10633 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10633&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10634 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10634&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10635 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10635&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10637 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10637&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10638 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10638&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10640 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10640&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10641 du 09 juillet 2014
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10641&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2004-0230
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0230
- Référence CVE CVE-2013-5211
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211
- Référence CVE CVE-2014-3815
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3815
- Référence CVE CVE-2014-3816
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3816
- Référence CVE CVE-2014-3817
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3817
- Référence CVE CVE-2014-3819
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3819
- Référence CVE CVE-2014-3821
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3821
- Référence CVE CVE-2014-3822
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3822

Gestion détaillée du document

10 juillet 2014 version initiale.