Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 15 juillet 2013
N° CERTA-2013-AVI-413

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Juniper Junos

Gestion du document

Référence	CERTA-2013-AVI-413
Titre	Multiples vulnérabilités dans Juniper Junos
Date de la première version	15 juillet 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10573 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10574 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10575 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10576 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10577 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10578 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10579 du 15 juillet 2013 Bulletin de sécurité Juniper JSA10580 du 15 juillet 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
- atteinte à la confidentialité des données

2 Systèmes affectés

- Juniper Junos OS version 10.4
- Juniper Junos OS version 11.4
- Juniper Junos OS version 12.1
- Juniper Junos OS version 12.1X44

3 Résumé

De multiples vulnérabilités ont été corrigées dans *Juniper Junos*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance 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 Juniper JSA10573 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10573
- Bulletin de sécurité Juniper JSA10574 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10574
- Bulletin de sécurité Juniper JSA10575 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10575
- Bulletin de sécurité Juniper JSA10576 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10576
- Bulletin de sécurité Juniper JSA10577 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10577
- Bulletin de sécurité Juniper JSA10578 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10578
- Bulletin de sécurité Juniper JSA10579 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10579
- Bulletin de sécurité Juniper JSA10580 du 15 juillet 2013
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10580
- Référence CVE CVE-2013-4684
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4684
- Référence CVE CVE-2013-4685
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4685
- Référence CVE CVE-2013-0166
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0166
- Référence CVE CVE-2013-0169
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169
- Référence CVE CVE-2013-4686
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4686
- Référence CVE CVE-2013-4687
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4687
- Référence CVE CVE-2013-4688
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4688
- Référence CVE CVE-2013-4690
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4690
- Référence CVE CVE-2013-1473
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1473

Gestion détaillée du document

15 juillet 2013 version initiale.