Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 octobre 2013
N° CERTA-2013-AVI-571

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Juniper Junos OS

Gestion du document

Référence	CERTA-2013-AVI-571
Titre	Multiples vulnérabilités dans Juniper Junos OS
Date de la première version	11 octobre 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10593 du 09 octobre 2013 Bulletin de sécurité Juniper JSA10594 du 09 octobre 2013 Bulletin de sécurité Juniper JSA10595 du 09 octobre 2013 Bulletin de sécurité Juniper JSA10596 du 09 octobre 2013 Bulletin de sécurité Juniper JSA10597 du 09 octobre 2013 Bulletin de sécurité Juniper JSA10598 du 09 octobre 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
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Juniper Junos OS 10.4
- Juniper Junos OS 11.4
- Juniper Junos OS 11.4X27
- Juniper Junos OS 12.1
- Juniper Junos OS 12.1X44
- Juniper Junos OS 12.1X45
- Juniper Junos OS 12.2
- Juniper Junos OS 12.3

– Juniper Junos OS 13.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Juniper Junos OS*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

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 JSA10593 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10593
- Bulletin de sécurité Juniper JSA10594 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10594
- Bulletin de sécurité Juniper JSA10595 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10595
- Bulletin de sécurité Juniper JSA10596 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10596
- Bulletin de sécurité Juniper JSA10597 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10598
- Bulletin de sécurité Juniper JSA10598 du 09 octobre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10598
- Référence CVE CVE-2010-2632
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2632
- Référence CVE CVE-2013-4689
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4689
- Référence CVE CVE-2013-6012
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6012
- Référence CVE CVE-2013-6013
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6013
- Référence CVE CVE-2013-6014
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6014
- Référence CVE CVE-2013-6015
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6015

Gestion détaillée du document

11 octobre 2013 version initiale.