Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 septembre 2013
N° CERTA-2013-AVI-527

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTA-2013-AVI-527
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	12 septembre 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10589 du 11 septembre 2013 Bulletin de sécurité Juniper JSA10590 du 11 septembre 2013 Bulletin de sécurité Juniper JSA10591 du 11 septembre 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
- injection de code indirecte à distance

2 Systèmes affectés

- Junos Pulse Secure Access Service (IVE) versions antérieures à 7.1r15
- Junos Pulse Secure Access Service (IVE) versions antérieures à 7.2r11
- Junos Pulse Secure Access Service (IVE) versions antérieures à 7.3r6
- Junos Pulse Secure Access Service (IVE) versions antérieures à 7.4r3
- Junos Pulse Access Control Service (UAC) versions antérieures à 4.1r8.1
- Junos Pulse Access Control Service (UAC) versions antérieures à 4.2r5.1
- Junos Pulse Access Control Service (UAC) versions antérieures à 4.3r6
- Junos Pulse Access Control Service (UAC) versions antérieures à 4.4r3

3 Résumé

De multiples vulnérabilités ont été corrigées dans *Produits Juniper*. Certaines d'entre 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 JSA10589 du 11 septembre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10589&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10590 du 11 septembre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10590&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10591 du 11 septembre 2013
  http://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10591&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2013-5649
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5649
- Référence CVE CVE-2013-5650
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5650
- Référence CVE CVE-2012-2131
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2131
- 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

Gestion détaillée du document

12 septembre 2013 version initiale.