Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 septembre 2013
N° CERTA-2013-AVI-508

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTA-2013-AVI-508
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	10 septembre 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10554 du 20 août 2013 Bulletin de sécurité Juniper JSA10582 du 20 août 2013 Bulletin de sécurité Juniper JSA10583 du 20 août 2013 Bulletin de sécurité Juniper JSA10584 du 20 août 2013 Bulletin de sécurité Juniper JSA10585 du 20 août 2013 Bulletin de sécurité Juniper JSA10586 du 20 août 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 l'intégrité des données
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 Systèmes affectés

- Juniper SA (IVE OS) versions antérieures à 7.1r13
- Juniper SA (IVE OS) versions antérieures à 7.2r7
- Juniper SA (IVE OS) versions antérieures à 7.3r2
- Juniper Junos Operating System

- Juniper JunosE Operating System
- Juniper ScreenOS
- Juniper STRM version 2010.0
- Juniper STRM version 2012.0
- Juniper STRM version 2012.1
- Juniper STRM version 2013.1
- Juniper NSM version 2010.3
- Juniper NSM version 2011.4
- Juniper NSM version 2012.1
- Juniper NSM version 2012.2
- Juniper Junos Space Software version 11.1
- Juniper Junos Space Software version 11.2
- Juniper Junos Space Software version 11.3
- Juniper Junos Space Software version 12.1
- Juniper Junos Space Software version 12.2
- Juniper Junos Space Software version 12.3
- Juniper Junos Space Appliance JA1500

3 Résumé

De multiples vulnérabilités ont été corrigées dans les 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 l'intégrité 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 JSA10554 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10554&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10582 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10582&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10583 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10583&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10584 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?cmid=no&page=content&id=JSA10584&cat=SIRT_1&actp=LIST&showDraft=false
- Bulletin de sécurité Juniper JSA10585 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10585&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10586 du 20 août 2013
  https://kb.juniper.net/InfoCenter/index?page=content&cmid=no&id=JSA10586&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2012-5460
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5460
- Référence CVE CVE-2013-0149
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0149
- Référence CVE CVE-2013-2970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2970
- Référence CVE CVE-2011-1473
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1473
- Référence CVE CVE-2011-3368
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368

- Référence CVE CVE-2011-4317
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4317
- Référence CVE CVE-2012-0053
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053
- Référence CVE CVE-2013-5095
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5095
- Référence CVE CVE-2013-5096
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5096
- Référence CVE CVE-2013-5097
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5097

Gestion détaillée du document

10 septembre 2013 version initiale.