

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits Juniper**

### Gestion du document

Référence	CERTFR-2017-AVI-111
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	12 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité JSA10776 Juniper du 12 avril 2017 Bulletin de sécurité JSA10777 Juniper du 12 avril 2017 Bulletin de sécurité JSA10778 Juniper du 12 avril 2017 Bulletin de sécurité JSA10780 Juniper du 12 avril 2017 Bulletin de sécurité JSA10781 Juniper du 12 avril 2017 Bulletin de sécurité JSA10783 Juniper du 12 avril 2017 Bulletin de sécurité JSA10784 Juniper du 12 avril 2017 Bulletin de sécurité JSA10785 Juniper du 12 avril 2017 Bulletin de sécurité JSA10786 Juniper du 12 avril 2017
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
- exécution de code arbitraire
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

## 2 - Systèmes affectés

- Juniper EX Series avec IPv6
- Junos OS
- Junos OS versions 15.1 et postérieures avec BGP

- NorthStar Controller Application antérieures à la version 2.1.0 SP1
- Juniper SRX, vSRX et J-Series avec le serveur DNS Proxy actif

### 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, une exécution de code arbitraire et un déni de service à distance.

### 4 - Solution

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

### 5 - Documentation

- Bulletin de sécurité JSA10781 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10781&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10781&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité SA10776 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10776&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10776&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10776 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10776&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10776&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10777 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10777&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10777&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10778 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10778&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10778&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10780 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10780&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10780&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10783 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10783&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10783&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10784 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10784&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10784&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10785 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10785&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10785&cat=SIRT_1&actp=LIST)
- Bulletin de sécurité JSA10786 Juniper du 12 avril 2017  
[https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10786&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10786&cat=SIRT_1&actp=LIST)
- Référence CVE CVE-2013-4450  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4450>
- Référence CVE CVE-2015-1349  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1349>
- Référence CVE CVE-2015-2808  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808>
- Référence CVE CVE-2015-3209  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3209>
- Référence CVE CVE-2015-3456  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3456>
- Référence CVE CVE-2015-4620  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4620>
- Référence CVE CVE-2015-5307  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5307>
- Référence CVE CVE-2015-5477  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5477>
- Référence CVE CVE-2015-7973  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7973>

- Référence CVE CVE-2015-7979  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7979>
- Référence CVE CVE-2015-8104  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8104>
- Référence CVE CVE-2015-8138  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8138>
- Référence CVE CVE-2015-8158  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8158>
- Référence CVE CVE-2016-1014  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1014>
- Référence CVE CVE-2016-1886  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1886>
- Référence CVE CVE-2016-2776  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2776>
- Référence CVE CVE-2016-7427  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7427>
- Référence CVE CVE-2016-7429  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7429>
- Référence CVE CVE-2016-7431  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7431>
- Référence CVE CVE-2016-8864  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8864>
- Référence CVE CVE-2016-9131  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9131>
- Référence CVE CVE-2016-9147  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9147>
- Référence CVE CVE-2016-9310  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9310>
- Référence CVE CVE-2016-9311  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9311>
- Référence CVE CVE-2016-9444  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9444>
- Référence CVE CVE-2017-2312  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2312>
- Référence CVE CVE-2017-2313  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2313>
- Référence CVE CVE-2017-2315  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2315>
- Référence CVE CVE-2017-2316  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2316>
- Référence CVE CVE-2017-2317  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2317>
- Référence CVE CVE-2017-2318  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2318>
- Référence CVE CVE-2017-2319  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2319>
- Référence CVE CVE-2017-2320  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2320>
- Référence CVE CVE-2017-2321  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2321>
- Référence CVE CVE-2017-2322  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2322>
- Référence CVE CVE-2017-2323  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2323>

- Référence CVE CVE-2017-2324  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2324>
- Référence CVE CVE-2017-2325  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2325>
- Référence CVE CVE-2017-2326  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2326>
- Référence CVE CVE-2017-2327  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2327>
- Référence CVE CVE-2017-2328  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2328>
- Référence CVE CVE-2017-2329  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2329>
- Référence CVE CVE-2017-2330  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2330>
- Référence CVE CVE-2017-2331  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2331>
- Référence CVE CVE-2017-2332  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2332>
- Référence CVE CVE-2017-2333  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2333>
- Référence CVE CVE-2017-2334  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2334>
- Référence CVE CVE-2017-2340  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2340>

## Gestion détaillée du document

12 avril 2017 version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-111>

---