Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 13 octobre 2016
N° CERTFR-2016-AVI-344

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTFR-2016-AVI-344
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	13 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10763 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10766 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10767 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10764 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10762 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10761 du 13 octobre 2016 Bulletin de sécurité Juniper JSA10760 du 13 octobre 2016
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
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Junos OS versions antérieures à 12.1X46-D60, 12.1X47-D45, 12.3R12, 12.3X48-D35, 13.2R9, 13.3R9, 14.1R7, 14.1X53-D40, 14.1X55-D35, 14.2R5, 15.1F4, 15.1R3, 15.1X49-D60, 15.1X53-D70, 16.1R1
- vMX versions antérieures à 14.1R8, 15.1F6 et 16.1
- Junos OS avec J-Web activé versions antérieures à 12.1X44-D60, 12.1X46-D40, 12.1X47-D30, 12.3R11, 12.3X48-D20, 13.2X51-D39, 13.2X51-D40, 13.3R9, 14.1R6, 14.2R6, 15.1R3, 15.1X49-D20 et 16.1R1

– Junos OS avec IPv6 versions antérieures à 11.4R13, 12.1X44-D45, 12.1X46-D30, 12.1X47-D20, 12.3R9 et 13.3R5

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 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 JSA10763 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10763&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10766 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10766&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10767 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10767&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10764 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10764&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10762 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10762&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10761 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10761&cat=SIRT_1&actp=LIST
– Bulletin de sécurité Juniper JSA10760 du 13 octobre 2016
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760&cat=SIRT_1&actp=LIST
– Référence CVE CVE-2016-4926
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4926
– Référence CVE CVE-2016-4927
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4927
– Référence CVE CVE-2016-4928
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4928
– Référence CVE CVE-2016-4929
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4929
– Référence CVE CVE-2016-4930
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4930
– Référence CVE CVE-2016-4931
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4931
– Référence CVE CVE-2011-0997
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0997
– Référence CVE CVE-2011-2748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2748
– Référence CVE CVE-2011-2749
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2749
– Référence CVE CVE-2012-3571
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3571
– Référence CVE CVE-2013-0169
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169
– Référence CVE CVE-2013-0791
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0791

- Référence CVE CVE-2013-1620
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1620
- Référence CVE CVE-2013-1739
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1739
- Référence CVE CVE-2013-1741
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1741
- Référence CVE CVE-2013-2596
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2596
- Référence CVE CVE-2013-5605
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5605
- Référence CVE CVE-2013-5606
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5606
- Référence CVE CVE-2013-5607
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5607
- Référence CVE CVE-2014-1490
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1490
- Référence CVE CVE-2014-1491
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1491
- Référence CVE CVE-2014-1492
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1492
- Référence CVE CVE-2014-1545
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1545
- Référence CVE CVE-2014-1568
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1568
- Référence CVE CVE-2015-1794
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1794
- Référence CVE CVE-2015-2151
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2151
- Référence CVE CVE-2015-3193
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3193
- Référence CVE CVE-2015-3194
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3194
- Référence CVE CVE-2015-3195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3195
- Référence CVE CVE-2015-3196
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3196
- Référence CVE CVE-2015-5364
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5364
- Référence CVE CVE-2015-5366
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5366
- Référence CVE CVE-2016-4921
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4921
- Référence CVE CVE-2016-4923
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4923
- Référence CVE CVE-2016-4925
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4925
- Référence CVE CVE-2016-4924
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4924
- Référence CVE CVE-2016-4922
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4922

Gestion détaillée du document

13 octobre 2016 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-2016-AVI-344