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 12 janvier 2017
N° CERTFR-2017-AVI-012

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTFR-2017-AVI-012
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	12 janvier 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité les produits Juniper JSA10770 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10773 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10774 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10768 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10769 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10771 du 11 janvier 2017 Bulletin de sécurité les produits Juniper JSA10772 du 11 janvier 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)

- non spécifié par l'éditeur
- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Junos Space versions antérieures à 16.1R1
- Juniper QFX3500, QFX3600, QFX5100, QFX5200, EX4300 et EX4600 exécutant Junos OS avec des versions antérieures à 4.1X53-D40, 15.1X53-D40, 15.1R2
- Juniper NSM3000, NSM4000 et NSMExpress sans le correctif de sécurité NSM Appliance Upgrade Package v3

- Juniper SRX Series Services Gateway chassis cluster avec PIM activé exécutant Junos OS avec des versions antérieures à 12.1X46-D65, 12.3X48-D40, 15.1X49-D60
- Tout produit Juniper avec DHCPv6 activé et exécutant Junos OS avec des versions antérieures à 11.4R13-S3, 12.1X46-D60, 12.3R12-S2, 12.3R13, 12.3X48-D40, 13.2X51-D40, 13.3R10, 14.1R8, 14.1X53-D12, 14.1X53-D35, 14.1X55-D35, 14.2R7, 15.1F6, 15.1R3, 15.1X49-D60, 15.1X53-D30, 16.1R1
- Tout produit Juniper avec RIP activé et exécutant Junos OS avec des versions antérieures à 12.1X46-D50, 12.1X47-D40, 12.3R13, 12.3X48-D30, 13.2X51-D40, 13.3R10, 14.1R8, 14.1X53-D35, 14.1X55-D35, 14.2R5, 15.1F6, 15.1R3, 15.1X49-D30, 15.1X49-D40, 15.1X53-D35, 16.1R1
- Tout produit Juniper exécutant Junos OS avec des versions antérieures à 12.1X46-D55, 12.1X47-D45, 12.3R13, 12.3X48-D35, 13.3R10, 14.1R8, 14.1X53-D40, 14.1X55-D35, 14.2R6, 15.1R1, 15.1X49-D20

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Juniper*. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance 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 les produits Juniper JSA10770 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10770&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10773 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10773&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10774 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10774&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10768 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10768&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10769 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10769&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10771 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10771&cat=SIRT_1&actp=LIST
- Bulletin de sécurité les produits Juniper JSA10772 du 11 janvier 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10772&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2015-5307
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5307
- Référence CVE CVE-2015-5352
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5352
- 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-2015-5600
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5600
- Référence CVE CVE-2015-6563
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6563
- Référence CVE CVE-2015-6564
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6564
- Référence CVE CVE-2015-6565
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6565

- Référence CVE CVE-2015-8104
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8104
- Référence CVE CVE-2015-8325
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8325
- Référence CVE CVE-2016-0777
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777
- Référence CVE CVE-2016-0778
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0778
- Référence CVE CVE-2016-1762
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1762
- Référence CVE CVE-2016-1833
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1833
- Référence CVE CVE-2016-1834
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1834
- Référence CVE CVE-2016-1835
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1835
- Référence CVE CVE-2016-1836
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1836
- Référence CVE CVE-2016-1837
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1837
- Référence CVE CVE-2016-1838
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1838
- Référence CVE CVE-2016-1839
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1839
- Référence CVE CVE-2016-1840
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1840
- Référence CVE CVE-2016-1907
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1907
- Référence CVE CVE-2016-3115
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3115
- Référence CVE CVE-2016-3627
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3627
- Référence CVE CVE-2016-3705
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3705
- Référence CVE CVE-2016-4447
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4447
- Référence CVE CVE-2016-4448
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4448
- Référence CVE CVE-2016-4449
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4449
- Référence CVE CVE-2016-5195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195
- Référence CVE CVE-2016-5387
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5387
- Référence CVE CVE-2016-5573
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5573
- Référence CVE CVE-2016-6515
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6515
- Référence CVE CVE-2016-6662
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6662
- Référence CVE CVE-2017-2300
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2300
- Référence CVE CVE-2017-2302
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2302

- Référence CVE CVE-2017-2303
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2303
- Référence CVE CVE-2017-2304
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2304
- Référence CVE CVE-2017-2305
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2305
- Référence CVE CVE-2017-2306
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2306
- Référence CVE CVE-2017-2307
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2307
- Référence CVE CVE-2017-2308
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2308
- Référence CVE CVE-2017-2309
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2309
- Référence CVE CVE-2017-2310
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2310
- Référence CVE CVE-2017-2311
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2311

Gestion détaillée du document

12 janvier 2017 version initiale.