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 14 avril 2016
N° CERTFR-2016-AVI-128

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTFR-2016-AVI-128
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	14 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10723 du 13 avril 2016 Bulletin de sécurité Juniper JSA10725 du 13 avril 2016 Bulletin de sécurité Juniper JSA10727 du 13 avril 2016 Bulletin de sécurité Juniper JSA10730 du 13 avril 2016 Bulletin de sécurité Juniper JSA10732 du 13 avril 2016 Bulletin de sécurité Juniper JSA10734 du 13 avril 2016 Bulletin de sécurité Juniper JSA10735 du 13 avril 2016 Bulletin de sécurité Juniper JSA10736 du 13 avril 2016 Bulletin de sécurité Juniper JSA10737 du 13 avril 2016 Bulletin de sécurité Juniper JSA10739 du 13 avril 2016 Bulletin de sécurité Juniper JSA10743 du 13 avril 2016 Bulletin de sécurité Juniper JSA10746 du 13 avril 2016 Bulletin de sécurité Juniper JSA10747 du 13 avril 2016 Bulletin de sécurité Juniper JSA10733 du 13 avril 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 l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- CTPOS versions antérieures à 7.1R2
- CTPOS versions antérieures à 7.2R1
- Junos OS versions antérieures à 12.1X44-D55
- Junos OS versions antérieures à 12.1X44-D60
- Junos OS versions antérieures à 12.1X46-D40
- Junos OS versions antérieures à 12.1X46-D45
- Junos OS versions antérieures à 12.1X47-D25
- Junos OS versions antérieures à 12.1X47-D30
- Junos OS versions antérieures à 12.1X47-D35
- Junos OS versions antérieures à 12.3R11
- Junos OS versions antérieures à 12.3R12
- Junos OS versions antérieures à 12.3R9
- Junos OS versions antérieures à 12.3X48-D20
- Junos OS versions antérieures à 12.3X48-D25
- Junos OS versions antérieures à 12.3X48-D30
- Junos OS versions antérieures à 12.3X50-D50
- Junos OS versions antérieures à 13.2R7
- Junos OS versions antérieures à 13.2R8
- Junos OS versions antérieures à 13.2R9
- Junos OS versions antérieures à 13.2X51-D39
- Junos OS versions antérieures à 13.2X51-D40
- Junos OS versions antérieures à 13.2X52-D30
- Junos OS versions antérieures à 13.3R6
- Junos OS versions antérieures à 13.3R7
- Junos OS versions antérieures à 13.3R8
- Junos OS versions antérieures à 13.3R9
- Junos OS versions antérieures à 14.1R4
- Junos OS versions antérieures à 14.1R6
- Junos OS versions antérieures à 14.1R7
- Junos OS versions antérieures à 14.1X53-D30
- Junos OS versions antérieures à 14.2R2
- Junos OS versions antérieures à 14.2R3
- Junos OS versions antérieures à 14.2R3-S4
- Junos OS versions antérieures à 14.2R4
- Junos OS versions antérieures à 14.2R4-S1
- Junos OS versions antérieures à 14.2R5
- Junos OS versions antérieures à 14.2R6
- Junos OS versions antérieures à 15.1F2
- Junos OS versions antérieures à 15.1F5
- Junos OS versions antérieures à 15.1R1
- Junos OS versions antérieures à 15.1R2
- Junos OS versions antérieures à 15.1R3
- Junos OS versions antérieures à 15.1X49-D10
- Junos OS versions antérieures à 15.1X49-D15
- Junos OS versions antérieures à 15.1X49-D20
- Junos OS versions antérieures à 15.1X49-D30
- Junos OS versions antérieures à 15.1X49-D40
- Junos OS versions antérieures à 15.1X53-D20
- Junos OS versions antérieures à 16.1R1
- Junos Space versions antérieures à 15.2R1
- ScreenOS versions antérieures à 6.3.0r22

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 JSA10723 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10723&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10725 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10725&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10727 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10727&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10730 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10730&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10732 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10732&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10734 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10734&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10735 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10735&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10736 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10736&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10737 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10737&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10739 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10739&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10743 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10743&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10746 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10746&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10747 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10747&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10733 du 13 avril 2016
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10733&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2004-0452
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0452
- Référence CVE CVE-2005-0448
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0448
- Référence CVE CVE-2008-2827
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2827
- Référence CVE CVE-2008-5302
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5302
- Référence CVE CVE-2008-5303
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5303
- Référence CVE CVE-2010-0212
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0212
- Référence CVE CVE-2010-1168
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1168

- Référence CVE CVE-2010-2761
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2761
- Référence CVE CVE-2010-3172
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3172
- Référence CVE CVE-2010-4410
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4410
- Référence CVE CVE-2011-1024
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1024
- Référence CVE CVE-2011-3597
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3597
- Référence CVE CVE-2012-5195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5195
- Référence CVE CVE-2012-5526
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5526
- Référence CVE CVE-2012-6329
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6329
- Référence CVE CVE-2013-1667
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1667
- Référence CVE CVE-2013-4449
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4449
- Référence CVE CVE-2014-0015
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0015
- Référence CVE CVE-2014-3613
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3613
- Référence CVE CVE-2014-3620
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3620
- Référence CVE CVE-2014-3707
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3707
- Référence CVE CVE-2014-8150
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8150
- Référence CVE CVE-2014-8151
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8151
- Référence CVE CVE-2015-1789
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1789
- Référence CVE CVE-2015-1790
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1790
- Référence CVE CVE-2015-1791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1791
- Référence CVE CVE-2015-2601
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2601
- Référence CVE CVE-2015-2613
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2613
- Référence CVE CVE-2015-2625
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2625
- Référence CVE CVE-2015-2659
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2659
- Référence CVE CVE-2015-2808
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808
- Référence CVE CVE-2015-3143
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3143
- Référence CVE CVE-2015-3144
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3144
- Référence CVE CVE-2015-3145
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3145

- Référence CVE CVE-2015-3148
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3148
- Référence CVE CVE-2015-3153
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3153
- Référence CVE CVE-2015-3183
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3183
- Référence CVE CVE-2015-3195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3195
- Référence CVE CVE-2015-4000
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
- Référence CVE CVE-2015-4748
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4748
- Référence CVE CVE-2015-4749
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4749
- 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-2016-1261
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1261
- Référence CVE CVE-2016-1264
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1264
- Référence CVE CVE-2016-1267
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1267
- Référence CVE CVE-2016-1268
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1268
- Référence CVE CVE-2016-1269
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1269
- Référence CVE CVE-2016-1270
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1270
- Référence CVE CVE-2016-1271
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1271
- Référence CVE CVE-2016-1273
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1273
- Référence CVE CVE-2016-1274
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1274

Gestion détaillée du document

14 avril 2016 version initiale.