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 avril 2015
N° CERTFR-2015-AVI-146

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTFR-2015-AVI-146
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	13 avril 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10679 du 07 avril 2015 Bulletin de sécurité Juniper JSA10680 du 07 avril 2015 Bulletin de sécurité Juniper JSA10678 du 07 avril 2015 Bulletin de sécurité Juniper JSA10677 du 07 avril 2015 Bulletin de sécurité Juniper JSA10676 du 07 avril 2015 Bulletin de sécurité Juniper JSA10675 du 07 avril 2015 Bulletin de sécurité Juniper JSA10674 du 07 avril 2015 Bulletin de sécurité Juniper JSA10673 du 07 avril 2015 Bulletin de sécurité Juniper JSA10672 du 07 avril 2015
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
- déni de service
- 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

2 - Systèmes affectés

- Juniper CTPOS versions antérieures à 6.6R5
- Juniper CTPOS versions antérieures à 7.0R4

- Juniper CTPOS versions antérieures à 7.1R1
- Juniper CTPView versions antérieures à 7.1R1
- Juniper IDP OS versions antérieures à 5.1r4
- Juniper Junos OS versions antérieures à 11.4R12
- Juniper Junos OS versions antérieures à 12.1X44-D50
- Juniper Junos OS versions antérieures à 12.1X46-D35
- Juniper Junos OS versions antérieures à 12.1X47-D25
- Juniper Junos OS versions antérieures à 12.2R9
- Juniper Junos OS versions antérieures à 12.2X50-D70
- Juniper Junos OS versions antérieures à 12.3R10
- Juniper Junos OS versions antérieures à 12.3R7
- Juniper Junos OS versions antérieures à 12.3R9
- Juniper Junos OS versions antérieures à 12.3X48-D10
- Juniper Junos OS versions antérieures à 13.1X50-D30
- Juniper Junos OS versions antérieures à 13.2R6
- Juniper Junos OS versions antérieures à 13.2R8
- Juniper Junos OS versions antérieures à 13.2X51-D30
- Juniper Junos OS versions antérieures à 13.2X52-D15
- Juniper Junos OS versions antérieures à 13.3R5
- Juniper Junos OS versions antérieures à 13.3R6
- Juniper Junos OS versions antérieures à 14.1R3
- Juniper Junos OS versions antérieures à 14.1R5
- Juniper Junos OS versions antérieures à 14.1X53-D10
- Juniper Junos OS versions antérieures à 14.2R1
- Juniper Junos OS versions antérieures à 14.2R3
- Juniper NSM versions antérieures à 2012.2R11
- Juniper NSM versions antérieures à 2012.2R12

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 déni de service.

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 JSA10679 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10679
- Bulletin de sécurité Juniper JSA10680 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10680
- Bulletin de sécurité Juniper JSA10678 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10678
- Bulletin de sécurité Juniper JSA10677 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10677
- Bulletin de sécurité Juniper JSA10676 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10676
- Bulletin de sécurité Juniper JSA10675 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10675

- Bulletin de sécurité Juniper JSA10674 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10674
- Bulletin de sécurité Juniper JSA10673 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10673
- Bulletin de sécurité Juniper JSA10672 du 07 avril 2015
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10672
- Référence CVE CVE-2009-3563
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3563
- Référence CVE CVE-2010-4478
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4478
- Référence CVE CVE-2011-0539
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0539
- Référence CVE CVE-2012-0814
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0814
- Référence CVE CVE-2012-2131
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2131
- Référence CVE CVE-2012-5195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5195
- Référence CVE CVE-2014-4478
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4478
- Référence CVE CVE-2014-6271
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
- Référence CVE CVE-2015-3006
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3006
- Référence CVE CVE-2015-3004
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3004
- Référence CVE CVE-2015-3003
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3003
- Référence CVE CVE-2014-3569
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3569
- Référence CVE CVE-2014-3570
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3570
- Référence CVE CVE-2014-3571
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3571
- Référence CVE CVE-2014-3572
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3572
- Référence CVE CVE-2014-8275
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8275
- Référence CVE CVE-2015-0204
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
- Référence CVE CVE-2015-0205
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0205
- Référence CVE CVE-2015-0206
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0206
- Référence CVE CVE-2015-0207
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0207
- Référence CVE CVE-2015-0208
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0208
- Référence CVE CVE-2015-0209
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0209
- Référence CVE CVE-2015-0285
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0285
- Référence CVE CVE-2015-0286
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0286

- Référence CVE CVE-2015-0287
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0287
- Référence CVE CVE-2015-0288
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0288
- Référence CVE CVE-2015-0289
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0289
- Référence CVE CVE-2015-0290
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0290
- Référence CVE CVE-2015-0291
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0291
- Référence CVE CVE-2015-0292
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0292
- Référence CVE CVE-2015-0293
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0293
- Référence CVE CVE-2015-1787
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1787
- Référence CVE CVE-2015-3005
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3005
- Référence CVE CVE-2015-3002
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3002
- Référence CVE CVE-2014-8500
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8500

Gestion détaillée du document

13 avril 2015 version initiale.