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 juillet 2017
N° CERTFR-2017-AVI-212

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Juniper

Gestion du document

Référence	CERTFR-2017-AVI-212
Titre	Multiples vulnérabilités dans les produits Juniper
Date de la première version	12 juillet 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Juniper JSA10775 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10779 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10782 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10787 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10789 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10790 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10791 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10792 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10793 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10794 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10795 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10796 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10797 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10798 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10799 du 12 juillet 2017 Bulletin de sécurité Juniper JSA10800 du 12 juillet 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 la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- CTPOS 7.0, 7.1, 7.2 et 7.3
- CTPView 7.1, 7.2 et 7.3
- ScreenOS versions antérieures à 6.3.0r24
- Junos OS toutes versions sans le dernier correctif de sécurité

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 Juniper JSA10775 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10775&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10779 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10779&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10782 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10782&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10787 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10787&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10789 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10789&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10790 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10790&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10791 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10791&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10792 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10792&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10793 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10793&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10794 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10794&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10795 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10795&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10796 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10796&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10797 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10797&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10798 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10798&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10799 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10799&cat=SIRT_1&actp=LIST
- Bulletin de sécurité Juniper JSA10800 du 12 juillet 2017
  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10800&cat=SIRT_1&actp=LIST
- Référence CVE CVE-2015-8138
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8138

- Référence CVE CVE-2016-1887
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1887
- Référence CVE CVE-2016-3074
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3074
- Référence CVE CVE-2016-7055
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7055
- Référence CVE CVE-2016-7426
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7426
- Référence CVE CVE-2016-7427
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7427
- Référence CVE CVE-2016-7428
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7428
- 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-2016-7433
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7433
- Référence CVE CVE-2016-7434
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7434
- 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-2016-9312
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9312
- Référence CVE CVE-2017-10605
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10605
- Référence CVE CVE-2017-2314
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2314
- Référence CVE CVE-2017-2335
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2335
- Référence CVE CVE-2017-2336
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2336
- Référence CVE CVE-2017-2337
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2337
- Référence CVE CVE-2017-2338
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2338
- Référence CVE CVE-2017-2339
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2339
- Référence CVE CVE-2017-2341
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2341
- Référence CVE CVE-2017-2342
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2342
- Référence CVE CVE-2017-2343
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2343
- Référence CVE CVE-2017-2344
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2344
- Référence CVE CVE-2017-2345
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2345
- Référence CVE CVE-2017-2346
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2346
- Référence CVE CVE-2017-2347
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2347

- Référence CVE CVE-2017-2348
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2348
- Référence CVE CVE-2017-3135
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3135
- Référence CVE CVE-2017-3731
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3731
- Référence CVE CVE-2017-3732
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3732

Gestion détaillée du document

12 juillet 2017 version initiale.