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 09 septembre 2016
N° CERTFR-2016-AVI-303

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Citrix

Gestion du document

Référence	CERTFR-2016-AVI-303
Titre	Multiples vulnérabilités dans les produits Citrix
Date de la première version	09 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Citrix CTX216642 du 08 septembre 2016 Bulletin de sécurité Citrix CTX216071 du 08 septembre 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

2 - Systèmes affectés

- Micrologiciel LOM versions antérieures à 3.21 pour solutions matérielles embarquées NetScaler MPX/SDX de type 8xxx et T1010, ainsi que CloudBridge CB2000 et CB3000
- Micrologiciel LOM versions antérieures à 3.39 pour solutions matérielles embarquées NetScaler MPX/SDX de type 11500/13500/14500/16500/18500/20500, 115xx, 17550/19550/20550/21550 et T1110, ainsi que CloudBridge CB4000 et CB5000
- Micrologiciel LOM versions antérieures à 3.24 pour solutions matérielles embarquées NetScaler de type 22xxx et T1200
- Micrologiciel LOM versions antérieures à 4.08 pour solutions matérielles embarquées NetScaler MPX/SDX de type 14xxx, 25xxx, T1120 et T1300
- Citrix XenServer version 7.0 sans le correctif de sécurité XS70E012
- Citrix XenServer version 6.5 SP1 sans le correctif de sécurité XS65ESP1038
- Citrix XenServer version 6.2 SP1 sans le correctif de sécurité XS62ESP1048

- Citrix XenServer version 6.1 sans le correctif de sécurité XS61E073
- Citrix XenServer version 6.0.2 sans le correctif de sécurité XS602E057
- Citrix XenServer version 6.0.2 Common Criteria sans le correctif de sécurité XS602ECC034
- Citrix XenServer version 6.0 sans le correctif de sécurité XS60E063

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Citrix*. 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 Citrix CTX216642 du 08 septembre 2016
  http://support.citrix.com/article/CTX216642
- Bulletin de sécurité Citrix CTX216071 du 08 septembre 2016
  http://support.citrix.com/article/CTX216071
- Référence CVE CVE-2013-3607
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3607
- Référence CVE CVE-2013-3608
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3608
- Référence CVE CVE-2013-3609
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3609
- Référence CVE CVE-2013-3619
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3619
- Référence CVE CVE-2013-3620
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3620
- Référence CVE CVE-2013-3621
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3621
- Référence CVE CVE-2013-3622
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3622
- Référence CVE CVE-2013-3623
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3623
- Référence CVE CVE-2013-4421
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4421
- Référence CVE CVE-2013-4434
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4434
- Référence CVE CVE-2014-3508
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3508
- Référence CVE CVE-2014-3509
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3509
- Référence CVE CVE-2014-3511
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3511
- Référence CVE CVE-2014-3566
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
- Référence CVE CVE-2014-3567
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3567
- Référence CVE CVE-2014-3568
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3568

- 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-2014-3572
  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-2015-0209
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0209
- 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-2015-0292
  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-2015-1788
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1788
- Référence CVE CVE-2015-1789
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1789
- Référence CVE CVE-2015-1791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1791
- Référence CVE CVE-2015-1792
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1792
- Référence CVE CVE-2015-4000
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
- Référence CVE CVE-2016-7092
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7092
- Référence CVE CVE-2016-7093
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7093
- Référence CVE CVE-2016-7094
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7094
- Référence CVE CVE-2016-7154
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7154

Gestion détaillée du document

09 septembre 2016 version initiale.