

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits BlueCoat

Gestion du document

Référence	CERTFR-2015-AVI-259
Titre	Multiples vulnérabilités dans les produits BlueCoat
Date de la première version	17 juin 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité BlueCoat SA92 du 16 juin 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
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Android Mobile Agent 1.x
- Client Connector
- CAS 1.1 versions antérieures à 1.1.5.6 et 1.2 versions antérieures 1.2.4.4
- Director 6.1 versions antérieures 6.1.19.1
- IntelligenceCenter 3.2 et 3.3
- BCAA 5.5 et 6.1
- CacheFlow 2.x et 3.x
- MAA 4.1 et 4.2
- MAG2
- Management Center versions antérieures 1.3.3.2
- ICSP 5.3
- NNP 5.2 et 5.3
- NSP 5.2 et 5.3
- OPIC

- PacketShaper 9.2
- PacketShaper S-Series 11.2, 11.3, et 11.4
- PolicyCenter 9.2
- ProxyAV 3.4 et 3.5
- ProxyClient 3.4
- SGOS 6.2 versions antérieures à 6.2.16.4, 6.5 versions antérieures à 6.5.7.5, et 6.6
- Reporter (Virtualized Reporter) 9.4
- SA 6.6, 7.0, et 7.1
- SSLV 3.7 et 3.8 versions antérieures à 3.8.2-418 et 3.8.3-120
- Unified Agent 4.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *BlueCoat*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité BlueCoat SA92 du 16 juin 2015
<https://bto.bluecoat.com/security-advisory/sa92>
- 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>

Gestion détaillée du document

17 juin 2015 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>

Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-259>
