

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Avaya Experience Portal

Gestion du document

Référence	CERTA-2014-AVI-008
Titre	Multiples vulnérabilités dans Avaya Experience Portal
Date de la première version	10 janvier 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya ASA-2012-448 du 08 janvier 2014 Bulletin de sécurité Avaya ASA-2012-479 du 08 janvier 2014 Bulletin de sécurité Avaya ASA-2012-482 du 08 janvier 2014 Bulletin de sécurité Avaya ASA-2012-371 du 08 janvier 2014 Bulletin de sécurité Avaya ASA-2013-041 du 08 janvier 2014 Bulletin de sécurité Avaya ASA-2012-444 du 08 janvier 2014
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 la confidentialité des données

2 - Systèmes affectés

Avaya Experience Portal versions antérieures à 7.0

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Avaya Experience Portal*. 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 Avaya ASA-2012-448 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100167395>
- Bulletin de sécurité Avaya ASA-2012-479 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100167733>
- Bulletin de sécurité Avaya ASA-2012-482 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100167760>
- Bulletin de sécurité Avaya ASA-2012-371 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100166061>
- Bulletin de sécurité Avaya ASA-2013-041 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100169684>
- Bulletin de sécurité Avaya ASA-2012-444 du 08 janvier 2014
<https://downloads.avaya.com/css/P8/documents/100167374>
- Référence CVE CVE-2011-1202
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1202>
- Référence CVE CVE-2011-3970
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3970>
- Référence CVE CVE-2012-1568
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1568>
- Référence CVE CVE-2012-2133
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2133>
- Référence CVE CVE-2012-2825
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2825>
- Référence CVE CVE-2012-2870
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2870>
- Référence CVE CVE-2012-2871
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2871>
- Référence CVE CVE-2012-2893
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2893>
- Référence CVE CVE-2012-3400
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3400>
- Référence CVE CVE-2012-3488
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3488>
- Référence CVE CVE-2012-3489
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3489>
- Référence CVE CVE-2012-3511
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3511>
- Référence CVE CVE-2012-3546
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3546>
- Référence CVE CVE-2012-4244
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4244>
- Référence CVE CVE-2012-4405
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4405>

Gestion détaillée du document

10 janvier 2014 version initiale.

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-008>
