

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans EMC Archer GRC

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-2013-AVI-293>

Gestion du document

Référence	CERTA-2013-AVI-293
Titre	Multiples vulnérabilités dans EMC Archer GRC
Date de la première version	07 mai 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité EMC ESA-2013-015 du 06 mai 2013
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
- contournement de la politique de sécurité
- injection de code indirecte à distance

2 Systèmes affectés

- RSA Archer version 5.x
- Archer Smart Suite Framework version 4.x

3 Résumé

De multiples vulnérabilités ont été corrigées dans *EMC Archer GRC*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une injection de code indirecte à distance (XSS).

4 Solution

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

5 Documentation

- Bulletin de sécurité EMC ESA-2013-015 du 06 mai 2013
<http://archives.neohapsis.com/archives/bugtraq/2013-05/att-0023/ESA-2013-015.txt>
- Référence CVE CVE-2013-0932
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0932>
- Référence CVE CVE-2013-0933
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0933>
- Référence CVE CVE-2013-0934
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0934>

Gestion détaillée du document

07 mai 2013 version initiale.