

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans EMC Documentum

Gestion du document

Référence	CERTFR-2014-AVI-362
Titre	Multiples vulnérabilités dans EMC Documentum
Date de la première version	20 août 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité EMC ESA-2014-073 du 20 août 2014 Bulletin de sécurité EMC ESA-2014-059 du 20 août 2014 Bulletin de sécurité EMC ESA-2014-067 du 20 août 2014 Bulletin de sécurité EMC ESA-2014-079 du 20 août 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
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- EMC Documentum Webtop
- EMC Documentum Administrator
- EMC Documentum WDK
- EMC Documentum Taskspace
- EMC Documentum Records Manager
- EMC Documentum Web Publisher
- EMC Documentum Digital Asset Manager
- EMC Documentum Engineering Plant Facilities Management Solution

- EMC Documentum Capital Projects
- EMC Documentum Records Client
- EMC Documentum D2
- EMC Documentum Content Server

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *EMC Documentum*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un contournement de la politique de sécurité 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 EMC ESA-2014-073 du 20 août 2014
<http://seclists.org/bugtraq/2014/Aug/att-90/ESA-2014-073.txt>
- Bulletin de sécurité EMC ESA-2014-059 du 20 août 2014
<http://seclists.org/bugtraq/2014/Aug/att-91/ESA-2014-059.txt>
- Bulletin de sécurité EMC ESA-2014-067 du 20 août 2014
<http://seclists.org/bugtraq/2014/Aug/att-92/ESA-2014-067.txt>
- Bulletin de sécurité EMC ESA-2014-079 du 20 août 2014
<http://seclists.org/bugtraq/2014/Aug/att-93/ESA-2014-079.txt>
- Référence CVE CVE-2014-4618
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4618>
- Référence CVE CVE-2014-2520
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2520>
- Référence CVE CVE-2014-2521
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2521>
- Référence CVE CVE-2014-0224
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>
- Référence CVE CVE-2014-0221
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0221>
- Référence CVE CVE-2014-0195
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0195>
- Référence CVE CVE-2014-0198
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0198>
- Référence CVE CVE-2010-5298
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5298>
- Référence CVE CVE-2014-3470
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3470>
- Référence CVE CVE-2014-0076
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0076>
- Référence CVE CVE-2014-2515
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2515>
- Référence CVE CVE-2014-2511
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2511>
- Référence CVE CVE-2014-2518
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2518>

Gestion détaillée du document

20 août 2014 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-2014-AVI-362>
