

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité dans Microsoft Exchange et Fast Search Server 2010

---

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-2012-ALE-004>

---

### Gestion du document

Référence	CERTA-2012-ALE-004-001
Titre	Vulnérabilité dans Microsoft Exchange et Fast Search Server 2010
Date de la première version	25 juillet 2012
Date de la dernière version	16 août 2012
Source(s)	Avis de sécurité Microsoft 2737111 du 24 juillet 2012
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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Microsoft Exchange Server 2007 Service Pack 3 ;
- Microsoft Exchange Server 2010 Service Pack 1 ;
- Microsoft Exchange Server 2010 Service Pack 2 ;
- Microsoft SharePoint Server 2010 Service Pack 1 ;
- FAST Search Server 2010 pour SharePoint.

## 3 Résumé

Une vulnérabilité a été découverte dans les bibliothèques « Oracle Outside In » utilisées par le service de transcodage de documents. Dans le cas le plus grave, un attaquant peut alors prendre le contrôle d'un serveur au moyen d'un fichier ou d'un message spécialement conçu.

## 4 Contournement provisoire

Se référer à l'avis de sécurité de sécurité Microsoft 2737111 (cf. section Documentation).

## 5 Solution

Appliquer le correctif de Microsoft MS12-058 (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS12-058 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/ms12-058>
- Avis du CERTA CERTA-2012-AVI-441 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-441/index.html>
- Avis de sécurité Microsoft 2737111 du 24 juillet 2012 :  
<http://technet.microsoft.com/fr-fr/security/advisory/2737111>  
<http://technet.microsoft.com/en-us/security/advisory/2737111>
- Bulletin de sécurité Oracle juillet 2012 :  
<http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html>
- Référence CVE CVE-2012-1766 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1766>
- Référence CVE CVE-2012-1767 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1767>
- Référence CVE CVE-2012-1768 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1768>
- Référence CVE CVE-2012-1769 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1769>
- Référence CVE CVE-2012-1770 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1770>
- Référence CVE CVE-2012-1771 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1771>
- Référence CVE CVE-2012-1772 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1772>
- Référence CVE CVE-2012-1773 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1773>
- Référence CVE CVE-2012-3106 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3106>
- Référence CVE CVE-2012-3107 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3107>
- Référence CVE CVE-2012-3108 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3108>
- Référence CVE CVE-2012-3109 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3109>
- Référence CVE CVE-2012-3110 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3110>

## Gestion détaillée du document

**25 juillet 2012** version initiale.

**16 août 2012** ajout de la solution.