

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Active Directory

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-2011-AVI-692>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2011-AVI-692 |
| Titre | Vulnérabilité dans Active Directory |
| Date de la première version | 14 décembre 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS11-095 du 13 décembre 2011 |
| 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

- Windows XP Service Pack 3 : Active Directory en mode application (ADAM) ;
- Windows XP Professionnel Édition x64 Service Pack 2 : Active Directory en mode application (ADAM) ;
- Windows Server 2003 Service Pack 2 : Active Directory ;
- Windows Server 2003 Service Pack 2 : Active Directory en mode application (ADAM) ;
- Windows Server 2003 Édition x64 Service Pack 2 : Active Directory ;
- Windows Server 2003 Édition x64 Service Pack 2 : Active Directory en mode application (ADAM) ;
- Windows Server 2003 avec SP2 pour systèmes Itanium : Active Directory ;
- Windows Vista Service Pack 2 : Active Directory Lightweight Directory Service (AD LDS) ;
- Windows Vista Édition x64 Service Pack 2 : Active Directory Lightweight Directory Service (AD LDS) ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 : Active Directory et Active Directory Lightweight Directory Service (AD LDS) ;
- Windows Server 2008 pour systèmes x64 Service Pack 2 : Active Directory et Active Directory Lightweight Directory Service (AD LDS) ;

- Windows 7 pour systèmes 32 bits et Windows 7 pour systèmes 32 bits Service Pack 1 : Active Directory Lightweight Directory Service (AD LDS) ;
- Windows 7 pour systèmes x64 et Windows 7 pour systèmes x64 Service Pack 1 : Active Directory Lightweight Directory Service (AD LDS) ;
- Windows Server 2008 R2 pour systèmes x64 et Windows Server 2008 R2 pour systèmes x64 Service Pack 1 : Active Directory et Active Directory Lightweight Directory Service (AD LDS).

3 Résumé

Une vulnérabilité a été corrigée dans Active Directory, Active Directory en mode application (ADAM) et Active Directory Lightweight Directory Service (AD LDS). Cette vulnérabilité peut être utilisée par une personne malveillante authentifiée sur un domaine Active Directory afin d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type corruption de mémoire a été corrigée dans Active Directory en mode application (ADAM) et Active Directory Lightweight Directory Service (AD LDS). Cette vulnérabilité peut être exploitée par une personne malveillante authentifiée sur un domaine Active Directory à l'aide d'une application spécialement conçue pour exécuter du code arbitraire pouvant potentiellement compromettre l'ensemble du domaine.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS11-095 du 13 décembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-095>
<http://technet.microsoft.com/en-us/security/bulletin/MS11-095>
- Référence CVE CVE-2011-3406 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3406>

Gestion détaillée du document

14 décembre 2011 version initiale.