

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Failles multiples dans la librairie ASN.1 de Microsoft

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-2004-AVI-032>

Gestion du document

Référence	CERTA-2004-AVI-032
Titre	Failles multiples dans la librairie ASN.1 de Microsoft
Date de la première version	11 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité de l'US-CERT
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 avec les privilèges SYSTEM. Les failles seraient identifiées depuis septembre 2003.

2 Systèmes affectés

Microsoft Windows NT4, 2000, XP et Server 2003.

3 Résumé

De multiples vulnérabilités dues à de mauvaises gestions des tampons ont été identifiées. Elles peuvent être utilisés, par un utilisateur mal intentionné, pour exécuter du code arbitraire à distance, sans même s'authentifier.

4 Description

ASN.1 (Abstract Syntax Notation One) est un langage standardisé servant à encoder des informations. Il est, par exemple, utilisé par le protocole SNMP ou les certificats X509 nécessaires pour le transport SSL/TLS et les messages chiffrés/signés S/MIME.

La bibliothèque Microsoft *msasn1.dll* en cause est utilisée par de nombreux services cryptographiques ou d'authentification sous Windows :

- certificats électroniques (X509),
- Kerberos,
- NTLMv2,
- SSL/TLS,...

5 Solution

Mettre les systèmes d'exploitation (serveurs comme clients) à jour, en se référant au bulletin du constructeur.

6 Documentation

- Avis Microsoft MS004-007 :
<http://microsoft.com/technet/security/bulletin/MS04-007.asp>
- Avis TA04-041A de l'US-CERT :
<http://www.us-cert.gov/cas/techalerts/TA04-041A.html>
- Référence CVE CAN-2003-0818 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818>

Gestion détaillée du document

11 février 2004 version initiale.