

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation de la vulnérabilité LSASS sous Windows : apparition du ver Sasser

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-ALE-007>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2004-ALE-007 |
| Titre | Exploitation de la vulnérabilité LSASS sous Windows : apparition du ver Sasser |
| Date de la première version | 02 mai 2004 |
| Date de la dernière version | – |
| Source(s) | |
| 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

Compromission de systèmes.

2 Systèmes affectés

- Microsoft Windows 2000 ;
- Microsoft Windows XP.

3 Résumé

Un ver permettant d'exploiter la vulnérabilité du service LSASS sur plusieurs plates-formes Microsoft Windows a fait son apparition.

4 Description

Le 14 avril 2004, le CERTA publiait l'avis CERTA-2004-AVI-126 (cf. section Documentation) relatif aux multiples vulnérabilités (mise en oeuvre du protocole PCT, faille service LSASS, etc.) présentes sur les systèmes d'exploitation Windows.

Depuis, de nombreux codes malicieux permettant d'exploiter plusieurs de ces vulnérabilités ont été largement diffusés et employés sur Internet.

Le 1er mai, un ver baptisé Sasser a fait son apparition. Ce ver infecte automatiquement tout système vulnérable connecté à Internet.

Le CERTA rappelle que ces codes malicieux n'ont aucun impact lorsque les systèmes sont mis à jour ou, à défaut, lorsque des mesures de contournement (désactivation des services inutiles, filtrage des ports au niveau des pare-feux) sont appliquées.

5 Solution

Appliquer au plus tôt le correctif fourni par Microsoft (cf avis MS04-11 de Microsoft).

Dans l'attente de l'application du correctif, filtrer les ports suivants :

- pour le protocole UDP, les ports 135, 137, 138 et 445 ;
- pour le protocole TCP, les ports 135, 139, 445 et 593 ;
- tout trafic entrant non sollicité.

6 Documentation

- Avis CERTA-2004-AVI-126 du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126/index.html>
- Bulletin de sécurité MS04-011 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>
- Avis de F-secure :
<http://www.f-secure.com/v-descs/sasser.shtml>
- Avis de Symantec :
<http://www.symantec.com/avcenter/venc/data/w32.sasser.worm.html>
- Avis de McAfee :
http://us.mcafee.com/virusinfo/default.asp?id=description&virus_k=125007
- avis de TrendMicro :
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.A

Gestion détaillée du document

02 mai 2004 version initiale.