

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du virus Bizex

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-002>

Gestion du document

Référence	CERTA-2004-ALE-002
Titre	Propagation du virus Bizex
Date de la première version	26 février 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 du système ;
- vol d'informations confidentielles.

2 Systèmes affectés

Plates-formes Microsoft Windows, sauf Windows 3.x.

3 Résumé

Le virus Bizex semble se propager actuellement, via les messageries instantanées ICQ.

4 Description

Le virus Bizex, qui semble se propager actuellement, utilise les messageries instantanées. Il invite le destinataire d'un message ICQ à cliquer sur un lien HTML. En exploitant plusieurs vulnérabilités de Windows et d'Internet Explorer, il s'installe sur le système de la victime.

Il capture ensuite les informations des fenêtres actives dont le nom appartient à la liste ci-dessous, stocke ces informations dans divers fichiers *.log* sur le système, et les transfère sur un serveur FTP.

Le virus se propage alors à tous les correspondants de la liste de contacts ICQ.

Concernant la vulnérabilité d'Internet Explorer :

- pour Symantec, il s'agit de la vulnérabilité *showhelp()* Cette vulnérabilité est décrite dans l'avis CERTA-2003-AVI-019 du 06 février 2003 (avis de sécurité Microsoft MS-03-004) ;
- pour McAfee, il s'agit d'une vulnérabilité corrigé par le patch ms03-040 (patch cumulatif). Ce patch a fait l'objet de l'alerte CERTA-2003-ALE-004 du 06 octobre 2003.

Le CERTA ne dispose pas encore de ce virus et ne peut pas valider ces informations.

Liste des fenêtres pour lesquelles le virus capture des informations :

- Acceso a Banca por Internet
- Accueil Bred.fr >Espace Bred.fr
- American Express UK - Personal Finance
- Banamex.com
- baNK
- Banque
- Banque en ligne
- Barclaycard Merchant Services
- Collegamento a Scigno
- Commercial Electronic Office Sign On
- Credit Lyonnais interacti
- CyberMUT
- e-gold Account Access
- E*TRADE Log On
- Home Page Banca Intesa
- LloydsTSB online - Welcome
- Merchant Administration
- Page d'accueil
- Secure User Area
- SUNCORP METWAY
- Tous les produits et services
- VeriSign Partner Manager
- VeriSign Personal Trust Service
- Wells Fargo - Small Business Home Page

5 Contournement provisoire

Pour limiter la fuite d'informations, filtrer le protocole FTP en sortie.

6 Solution

- Appliquer tous les correctifs sur les systèmes ;
- mettre à jour le système antivirus.

7 Documentation

- Avis de sécurité CERTA-2003-AVI-019 du 06 février 2003 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-019/index.html>

- Avis de sécurité de Microsoft MS03-004 :
<http://www.microsoft.com/technet/security/bulletin/ms03-004.asp>
- Avis de sécurité de Microsoft MS03-040 :
<http://www.microsoft.com/technet/security/bulletin/ms03-040.asp>
- Alerte de sécurité CERTA-2003-ALE-004 du 06 octobre 2003 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-004/index.html>
- Bulletin de sécurité de Kaspersky :
<http://www.kaspersky.com/news.html?id=4277566>
- Bulletin de sécurité de McAfee :
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101044
- Bulletin de sécurité de Symantec :
<http://securityresponse.symantec.com/avcenter/venc/data/w32.bizex.worm.html>
- Analyse du virus :
<http://www.viruslist.com/eng/viruslist.html?id=1029528>
- Recommandation du CERTA sur l'usage de la messagerie instantanée ou de l'IRC :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-001/index.html>

Gestion détaillée du document

26 février 2004 version initiale.