Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 19 août 2003
N° CERTA-2003-ALE-002-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation d'une faille de Windows RPC

Gestion du document

Référence	CERTA-2003-ALE-002-002
Titre	Exploitation d'une faille de Windows RPC
Date de la première version	01 août 2003
Date de la dernière version	19 août 2003
Source(s)	Avis CA-2003-19 du CERT/CC
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.

2 Systèmes affectés

- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0 Terminal Services Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Windows Server 2003.

3 Résumé

Des programmes permettant d'exploiter la faille de l'interface RPC sous Windows décrite dans l'avis CERTA-2003-AVI-111 du CERTA sont largement diffusés et employés sur l'Internet.

Le 11 août un ver nommé Blaster (W32/Blaster) a fait son apparition. Depuis, d'autres variantes de ce ver sont apparues.

4 Description

La faille de l'interface RPC permet en particulier à un utilisateur distant mal intentionné d'obtenir un *shell* et d'exécuter du code arbitraire avec les droits du compte *Local System*.

Des programmes exploitant cette vulnérabilité, ainsi que des scanners permettant de détecter les machines vulnérables ont été largement diffusés sur l'Internet.

L'exploitation de cette vulnérabilité peut engendrer certains dysfonctionnements sur la machine cible.

4.1 Ver W32/Blaster

Le ver nommé « W32/Blaster » exploite également cette vulnérabilité sur Windows 2000 et XP : une copie du fichier `msblast.exe` est déposé sur la machine cible vulnérable depuis une machine déjà infectée, puis cette même machine procède à son tour à la recherche de systèmes vulnérables sur le port 135. Le ver a également la capacité de réaliser un déni de service de type « tcp syn flood » sur le site http://www.windowsupdate.com.

Il est possible de savoir si une machine est infectée par la présence de la clef de registre `Software\Microsoft\Windows\CurrentVersion\Run\windows auto update=msblast.exe`.

Bloquer le trafic vers les ports 4444/TCP et 69/UDP permet de freiner la propagation de ce ver.

4.2 Ver W32/Nachi, W32/Welchia

Le ver nommé « W32/Nachi » ou « W32/Welchia » (selon l'éditeur de l'antivirus) exploite également cette vulnérabilité, ainsi que la vulnérabilité de WebDav décrite dans l'avis CERTA-2003-AVI-050. Le ver recherche les machines ayant le port 135/tcp ouvert, puis envoie un paquet ICMP ECHO REQUEST avec un champ données rempli de 'A'. En cas de réponse à ce paquet, le ver infecte la machine. Une fois la machine compromise, le ver crée un *shell* sur le port 707/tcp et utilise TFTP (port 69/udp) pour les téléchargements. Le ver tente ensuite d'éliminer le ver Blaster s'il est présent sur la machine, et télécharge les correctifs de Microsoft (versions chinoises, coréennes et anglaises) pour Windows 2000 et Windows XP.
Le ver s'efface automatiquement le 1er janvier 2004.

5 Contournement provisoire

Pour éviter les attaques venant de l'extérieur, filtrer les ports 135 à 139 et 445 en TCP et en UDP.

6 Solution

Appliquer au plus tôt le correctif fourni par Microsoft suivant la version du système d'exploitation.

7 Documentation

- Avis CERTA-2003-AVI-111 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-111/index.html
- Avis CA-2003-19 du CERT/CC :
  http://www.cert.org/advisories/CA-2003-19.html
- Bulletin de sécurité MS03-026 de Microsoft :
  http://www.microsoft.com/security/security_bulletins/ms03-026.asp

Ver W32/Blaster :

- Avis CA-2003-20 du CERT/CC :
  http://www.cert.org/advisories/CA-2003-20.html
- Avis de F-secure :
  http://www.f-secure.com/v-descs/msblast.shtml

- Avis de Symantec :
  http://www.symantec.com/avcenter/venc/data/w32.blaster.worm.html
- Avis de Mcafee :
  http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=10054
- Avis de Sophos :
  http://www.sophos.com/virusinfo/analyses/w32blastera.html
- Avis de TrendMicro :
  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

Ver W32/Nachi et W32/Welchia :

- Avis de Network Associates :
  http://vil.nai.com/vil/content/v_100559.htm
- Avis de F-Secure :
  http://www.f-secure.com/v-descs/welchi.shtml
- Avis de Symantec :
  http://www.symantec.com/avcenter/venc/data/w32.welchia.worm.html
- Avis de Sophos :
  http://www.sophos.com/virusinfo/analyses/w32nachia.html
- Avis de TrendMicro :
  http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.D

Gestion détaillée du document

01 août 2003 version initiale ;
12 août 2003 apparition du ver W32/Blaster.
19 août 2003 apparition du ver W32/Nachi, W32/Welchia.