Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 novembre 2001
N° CERTA-2001-AVI-010-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le serveur DNS BIND

Gestion du document

Référence	CERTA-2001-AVI-010-001
Titre	Multiples vulnérabilités dans le serveur DNS BIND
Date de la première version	30 novembre 2001
Date de la dernière version	30 janvier 2001
Source(s)	Avis du CERT/CC CA-2001-02 du 29/01/2001
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Accès distant avec les privilèges du super-utilisateur.
- Divulgation d'informations système (variables d'environnement).
- Déni de service induisant un déni de service pour les autres protocoles internet (messagerie, serveur et navigation web, ...).

Les précédentes failles de BIND (12 avis du CERT/CC depuis 1997) ont systématiquement donné lieu à des exploitations massives et prolongées.

2 Systèmes affectés

Majorité des systèmes Unix, systèmes Windows NT utilisant BIND.

3 Résumé

Quatre vulnérabilités majeures ont été découvertes dans le code du serveur DNS BIND, développé par l'Internet Software Consortium (ISC), permettant à un utilisateur distant de prendre le contrôle de la machine hôte.

Il existe une interrogation DNS permettant de connaître la version de BIND tournant à une adresse IP donnée, et donc, pour un utilisateur hostile, de conclure sur la vulnérabilité à exploiter.

4 Description

- Il existe un débordement de pile dans la fonction TSIG (authentification de transaction par clef secrète partagée - RFC 2845) qui permet à un utilisateur distant mal intentionné d'exécuter du code sur la machine serveur et par conséquent d'obtenir les privilèges du super-utilisateur ou un déni de service (versions 8.x.x).
- De plus il y a deux débordements de pile supplémentaires dans l'interface avec la journalisation système ayant les mêmes conséquences que précédemment (versions 4.x.x).
- La dernière vulnérabilité permet à un utilisateur distant de lire la pile du programme permettant éventuellement de lire des variables d'environnement ou du programme. Ces informations peuvent aider au développement d'exploits concernant les trois débordements de pile précédents (versions 4.x.x et 8.x.x).

5 Contournement provisoire

Il n'existe pas de contournement provisoire, le DNS étant indispensable au fonctionnement d'internet, il est nécessaire de procéder aux mises à jour.

6 Solution

Mettre à jour le serveur BIND :

- Branche 4.x.x (n'est plus activement maintenue) : évoluer vers la version 4.9.8
  ftp://ftp.isc.org/isc/bind/src/DEPRECATED/4.9.8/bind-498-REL.tar.gz
- Branche 8.x.x : évoluer vers la version 8.2.3
  ftp://ftp.isc.org/isc/bind/src/8.2.3/bind-src.tar.gz

Nota : il existe une nouvelle branche de développement visant à implémenter le DNSSEC, dont la dernière version est la 9.1, mais elle est loin d'avoir toutes fonctionnalités de la branche 8.x.x. Son installation n'est pas recommandée.

Correctifs de certains vendeurs (liste non exhaustive)

Caldera Linux

- OpenLinux 2.3, archive RPM sous :
  ftp://calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/
- eServer 2.3.1, archive RPM sous :
  ftp://calderasystems.com/pub/updates/eServer/2.3/current/RPMS/
- eDesktop 2.4, archive RPM sous :
  ftp://calderasystems.com/pub/updates/eDesktop/2.4/current/RPMS/

Mandrake Linux

Suivre les directives depuis la page suivante pour les versions 6.0, 6.1, 7.0, 7.1, 7.2 et Corporate Server 1.0.1 :
http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-017.php3

Trustix

http://www.trustix.net/pub/Trustix/updates

Debian

Les paquetages pour la version 2.2 sont disponibles selon l'architecture sous :
http://security.debian.org/dists/stable/updates/main/

TurboLinux

http://www.turbolinux.com/pipermail/tl-security-announce/2001-February/000034.html

SuSE Linux

http://www.suse.com/de/support/security/2001_03_bind8_txt.txt

Conectiva Linux

http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000377

RedHat Linux

http://www.redhat.com/support/errata/RHSA-2001-007.html

Slackware Linux

http://archives.neohapsis.com/archives/bugtraq/2001-01/0477.html

Immunix

http://archives.neohapsis.com/archives/linux/immunix/2001-q1/0046.html

Compaq Tru64

http://archives.neohapsis.com/archives/compaq/2001-q1/0074.html

HP-UX

http://archives.neohapsis.com/archives/hp/2001-q1/0069.html

IBM AIX

http://archives.neohapsis.com/archives/aix/2001-q1/0008.html

Sun Solaris

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=salert%2F26965

NetBSD

ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2001-001.txt.asc

FreeBSD

ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc

OpenBSD

http://archives.neohapsis.com/archives/openbsd/2001-02/0191.html

7 Documentation

- Avis CA-2001-02 du CERT/CC
  http://www.cert.org/advisories/CA-2001-02.html
- Avis des laboratoires COVERT de PGP security
  http://www.pgp.com/research/covert/advisories/047.asp

Gestion détaillée du document

30 janvier 2001 version initiale.
30 novembre 2001 mise à jour des correctifs des vendeurs.