Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2001
N° CERTA-2001-ALE-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Prolifération du ver Li0n

Gestion du document

Référence	CERTA-2001-ALE-003
Titre	Prolifération du ver Li0n
Date de la première version	26 mars 2001
Date de la dernière version	–
Source(s)	Bulletin du SANS Institute
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 serveur de noms (DNS)

2 Systèmes affectés

Linux avec Bind 8.2, 8.2-P1, 8.2.1, 8.2.2-Px

3 Résumé

Un nouveau ver, très proche du ver Ramen (CERTA-2001-ALE-001) , appelé Li0n, exploite la dernière vulnérabilité de Bind pour compromettre les machines Linux.

4 Description

Le 29 janvier 2001, une nouvelle vulnérabilité de Bind, appelée «vulnérabilité TSIG» était annoncée (Référence CERTA-2001-AVI-010).

Cette vulnérabilité est aujourd'hui exploitée par un ver appelé Li0n. Lorsqu'une machine est compromise par ce ver, un grand nombre de fichiers est installé. Parmi eux se trouvent :

- Le rootkit t0rnkit (reprogrammation de du, find, ifconfig, login, ls, ps, netstat, top, in.telnetd, in.fingerd, pstree);
- Le fichier /etc/ttyhash qui contient un mot de passe chiffré ;
- Le fichier /usr/sbin/nscd qui est en fait une version modifiée de sshd ;
- Le fichier randb qui scanne l'équivalent d'une classe B à la recherche de versions de Bind vulnérables ;
- Des outils de compromission automatique des machines trouvées vulnérables par rand ;
- Le fichier mjy qui efface les traces dans les fichiers de logs.

De plus, le fichier /etc/host.deny est effacé, les fichiers /etc/passwd et /etc/shadow sont envoyés par mèl à une adresse en Chine.

Enfin, Li0n installe quelques portes dérobées (typiquement sur les ports 60008/tcp, 33567/tcp et 33568/tcp, mais ces ports peuvent être facilement modifiés).

5 Contournement provisoire

Filtrer au niveau du garde barrière les ports supérieurs à 1024 non explicitement autorisés sur les machines de votre réseau.

Sans Institute propose sur son site un utilitaire permettant de déceler la présence de Li0n :
http://www.sans.org/y2k/lionfind-01.1.tar.gz

6 Solution

Au cas où votre mise à jour de Bind n'ai pas encore été faite, reportez vous à l'avis CERTA-2001-AVI-010 afin d'avoir la liste des correctifs.

7 Documentation

- Bulletin SANS :
  http://www.sans.prg/y2k/lion.htm
- CERTA-2001-ALE-001 ;
- CERTA-2001-AVI-010.

Gestion détaillée du document

26 mars 2001 version initiale.