

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver Ramen sous Linux.

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-2001-ALE-001>

Gestion du document

Référence	CERTA-2001-ALE-001
Titre	Propagation du ver Ramen sous Linux.
Date de la première version	19 janvier 2001
Date de la dernière version	–
Source(s)	Avis IN-2001-01 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

- Propagation de ver;
- défiguration de sites web;
- dénis de services;
- destruction de fichiers de configuration;
- compromission.

2 Systèmes affectés

- Linux RedHat 6.2 et 7.0, Mandrake 6.0 à 7.1 à priori (liste non-exhaustive).
- Mais, toute autre machine (actuellement ayant une architecture i386) sur laquelle n'ont pas été appliqués les correctifs concernant Wu-FTPd (cf. CERTA-2000-ALE-010), `rpc.statd` (cf. CERTA-2000-AVI-039) et `LPRng` (cf. CERTA-2000-AVI-087) est susceptible d'être attaquée.
- Une modification du ver n'est pas impossible, tout système n'étant pas à jour est susceptible d'être corrompu.

3 Résumé

Le ver nommé Ramen se propage via les vulnérabilités citées ci-dessus, détériore les configurations des systèmes et défigure les sites web hébergés par les machines qu'il a compromises.

4 Description

Le ver Ramen est basé sur des *scripts shells* accompagnés de fichiers binaires qui utilisent les vulnérabilités de Wu-FTPd (cf. CERTA-2000-ALE-010), *rpc.statd* (cf. CERTA-2000-AVI-039) et LPRng (cf. CERTA-2000-AVI-087) pour se propager.

Lorsqu'il a obtenu les privilèges *root* sur la machine victime, il va télécharger, depuis une machine déjà compromise, le *toolkit* lui permettant de compromettre d'autres machines après avoir fait les actions qui suivent :

- modifie certains fichiers de configuration (*/etc/hosts.deny*, */etc/rc.d/rc.sysinit*, ...),
 - crée un répertoire contenant un fichier (*/usr/src/.pooop/myip*) ainsi qu'un programme (un serveur nommé */usr/sbin/asp*),
 - détruit des fichiers (*/usr/sbin/rpc.statd* et */sbin/rpc.statd*)
 - et remplace la page *index.html* du serveur web hébergé par son hôte (si il existe) par sa propre version de *index.html*. Il s'agit d'une image d'un sachet de pâtes accompagnée du message : « Hackers looooooooooooooooooove noodles. ».
- Pour les systèmes utilisant le fichier */etc/inetd.conf*, le ver y ajoute le service */usr/sbin/asp* et redémarre le démon *inetd*.
 - Pour les systèmes ne possédant pas de fichier */etc/inetd.conf*, le même service est ajouté dans le fichier */etc/xinetd.conf* et le démon *xinetd* et redémarré.

Ceci permet au ver d'écouter sur le port 27374.

- Enfin, le *toolkit* (*/usr/src/.pooop/ramen.tgz*) installé, il lance un scan sur le réseau pour compromettre d'autres victimes.

5 Contournement provisoire

Un garde-barrière refusant l'accès entrant ou sortant sur le port 27374/TCP empêchera le téléchargement, dans un sens comme dans l'autre, du *toolkit* et donc la propagation du ver.

6 Solution

Appliquer tous les correctifs fournis par l'éditeur des systèmes, notamment (dans l'immédiat) ceux indiqués dans les documents émis par le CERTA concernant Wu-FTPd (cf. CERTA-2000-ALE-010), *rpc.statd* (cf. CERTA-2000-AVI-039) et LPRng (cf. CERTA-2000-AVI-087).

7 Documentation

Avis du CERT/CC :

http://www.cert.org/incident_notes/IN-2001-01.html

Gestion détaillée du document

19 janvier 2001 version initiale.