



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2002
N° CERTA-2002-AVI-034-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du paquetage ucd-snmp

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-2002-AVI-034>

Gestion du document

Référence	CERTA-2002-AVI-034-001
Titre	Multiples vulnérabilités du paquetage ucd-snmp
Date de la première version	18 février 2002
Date de la dernière version	23 mai 2002
Source(s)	Avis RHSA-2001:163 de RedHat
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

- Elévation de privilèges ;
- déni de service.

2 Systèmes affectés

Ucd-snmp versions 4.2.2 et antérieures.

3 Résumé

Le paquetage ucd-snmp comprend un ensemble d'outils (agent SNMP, génération et capture de TRAP, etc) très utilisés sous Linux.

De multiples vulnérabilités présentes dans le paquetage ucd-snmp permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance avec les privilèges de l'administrateur root.

4 Description

Des tests effectués par l'université finlandaise d'Oulu ont mis en évidence la présence de vulnérabilités dans les routines de décodage et de traitement des messages SNMP dans de nombreuses implémentations (se référer au bulletin d'alerte CERTA-2002-ALE-004 du CERTA).

L'exploitation de vulnérabilités, de type débordement de mémoire, présentes dans le paquetage ucd-snmp, permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

5 Contournement provisoire

- Ne démarrer l'agent SNMP que si celui-ci est nécessaire ;
- ne pas utiliser les noms de communautés positionnés lors de l'installation par défaut ;
- filtrer les ports 161/udp et 162/udp utilisés par le protocole SNMP V1 au niveau du garde-barrière afin d'empêcher l'exploitation de ces vulnérabilités depuis l'Internet.

6 Solution

Il est conseillé d'appliquer les correctifs des différents éditeurs (consultez la section Documentation).

7 Documentation

- Avis de sécurité RHSA-2001:163 de RedHat :
<http://www.redhat.com/support/errata/RHSA-2001-163.html>
- Avis de sécurité MDKSA-2002:014 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2001/MDKSA-2002-014.php>
- Avis de sécurité DSA-111-1 de Debian :
<http://www.debian.org/security/2002/dsa-111>
- Avis de sécurité FreeBSD-SA-02:11 de FreeBSD :
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:11.snmp.asc>
- Avis de sécurité SuSE-SA:2002:12 de SuSE :
http://www.suse.com/de/support/security/2002_012_ucdsnmp_txt.html

Gestion détaillée du document

18 février 2002 version initiale.

23 mai 2002 ajout référence à l'avis SuSE dans la section documentation.