Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 avril 2004
N° CERTA-2003-AVI-110-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des pilotes de carte réseau Ethernet

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-2003-AVI-110

Gestion du document

Référence	CERTA-2003-AVI-110-001
Titre	Vulnérabilité des pilotes de carte réseau Ethernet
Date de la première version	15 juillet 2003
Date de la dernière version	06 avril 2004
Source(s)	Note de vulnérabilité VU#412115 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

Divulgation d'informations.

2 Systèmes affectés

Les pilotes des cartes réseau Ethernet des distributions suivantes peuvent être vulnérables :

- Debian ;
- EnGarde Secure Linux ;
- HP-UX ;
- Mandrake ;
- Red Hat ;
- Sun OS ;
- SGI IRIX.

De plus, des pilotes de carte ont été identifiés comme vulnérables :

- les pilotes NDIS2 d'Intel versions antérieures à 3.2 sous Windows et OS/2 sont vulnérables ;
- les pilotes ODI d'Intel versions antérieures à 2.13 sous Novell sont vulnérables ;
- le pilote de DocuColor 1632/2240 de Xerox est vulnérable.

D'autres pilotes peuvent être affectés par cette vulnérabilité.

3 Résumé

Un utilisateur mal intentionné peut voler des informations contenues en mémoire en utilisant des trames Ethernet avec un champ données de petite taille.

4 Description

Les paquets Ethernet ont un champ données d'une taille minimum de 46 octets. La RFC 1042 (Request For Comments) spécifie que si le champ données du paquet fait moins de 46 octets, celui-ci devrait être augmenté de zéros afin d'obtenir la taille minimum. Néanmoins, certains pilotes de carte réseau Ethernet utilisent des informations contenues en mémoire pour réaliser le remplissage du champ données.

Un utilisateur mal intentionné peut ainsi voler des informations contenues en mémoire en envoyant des trames Ethernet avec un champ données de trop petite taille.

5 Solution

Appliquer le correctif proposé soit par le revendeur de la distribution utilisée, soit par le revendeur de la carte.

6 Documentation

- Note de vulnérabilité VU#412115 du CERT/CC :
  http://www.kb.cert.org/vuls/id/412115
- référence CVE CAN-2003-0001 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0001
- RFC 1042 :
  http://www.ietf.org/rfc/rfc1042.txt
- avis HPSBUX0305-261 de HP :
  http://support.itrc.hp.com http://support.itrc.hp.comhttp://support.itrc.hp.com
- avis de sécurité DSA-311-1 de Debian :
  http://www.debian.org/security/2003/dsa-311
- avis de sécurité ESA-20030318-009 de EnGarde Secure Linux :
  http://www.linuxsecurity.com/advisories/engarde_advisory-2976.html
- avis de sécurité MDKSA-2003:039 de MandrakeSoft :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:039
- avis Red Hat Enterprise Linux :
  http://rhn.redhat.com/errata/RHSA-2003-103.html
- avis Red Hat (noyau versions 2.4) :
  http://rhn.redhat.com/errata/RHSA-2003-025.html
- avis Red Hat (noyau versions 2.2) :
  http://rhn.redhat.com/errata/RHSA-2003-088.html
- avis de sécurité SGI IRIX :
  http://patches.sgi.com/support/free/security/advisories/20030601-01-l.asc
- réponse à la note de vulnérabilité VU#412115 du CERT/CC par Xerox :
  http://www.xerox.com/security

Gestion détaillée du document

15 juillet 2003 version initiale.
06 avril 2004 ajout avis de sécurité SGI.