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 juillet 2004
N° CERTA-2004-AVI-171-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Neon

Gestion du document

Référence	CERTA-2004-AVI-171-005
Titre	Vulnérabilité de Neon
Date de la première version	21 mai 2004
Date de la dernière version	30 juillet 2004
Source(s) Avis de sécurité e-matters	
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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Les versions de `neon` antérieures à la version 0.24.6.

3 Résumé

Une vulnérabilité présente dans `Neon` permet à un utilisateur mal intentionné, via une date malicieusement construite, d'exécuter du code arbitraire à distance ou de réaliser un déni de service sur le système vulnérable.

4 Description

Neon est une bibliothèque WebDAV utilisée par un grand nombre d'applications WebDAV.

Une vulnérabilité de type « buffer overflow » dans la fonction `ne_rfc1036_parse()` de `Neon`, utilisée pour le traitement de la date, permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire.

5 Solution

Appliquer la mise à jour (cf. section documentation).

6 Documentation

- Bulletin de sécurité e-matters :
  http://security.e-matters.de/advisories/062004.html
- Bulletin de sécurité Mandrake MDKSA-2004:049 du 19 mai 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:049
- Bulletin de sécurité Mandrake MDKSA-2004:078 du 29 juillet 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:078
- Bulletin de sécurité RedHat RHSA-2004-191 du 19 mai 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-191.html
- Bulletin de sécurité Debian DSA-506 du 19 mai 2004 :
  http://www.debian.org/security/2004/dsa-506
- Bulletin de sécurité Debian DSA-507 du 19 mai 2004 :
  http://www.debian.org/security/2004/dsa-507
- Bulletin de sécurité GLSA 200405-13 de Gentoo du 20 mai 2004 pour neon :
  http://www.gentoo.org/security/en/glsa/glsa-200405-13.xml
- Bulletin de sécurité GLSA 200405-25 de Gentoo du 30 mai 2004 pour tla :
  http://www.gentoo.org/security/en/glsa/glsa-200405-25.xml
- Bulletin de sécurité GLSA 200406-03 de Gentoo du 05 juin 2004 pour sitecopy :
  http://www.gentoo.org/security/en/glsa/glsa-200406-03.xml
- Bulletin de sécurité SUSE SuSE-SA:2004:015 du 09 juin 2004 pour tla, sitecopy et cadaver :
  http://www.suse.com/de/security/2004_15_cvs.html
- Bulletin de sécurité FreeBSD pour neon du 19 mai 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité pour le paquetage OpenBSD neon et cadaver du 19 mai 2004 :
  http://www.vuxml.org/openbsd/
- Mise à jour de sécurité du paquetage NetBSD neon :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/neon/README.html
- Référence CVE CAN-2004-0398 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0398

Gestion détaillée du document

21 mai 2004 version initiale.
24 mai 2004 ajout de l'avis Debian cadaver et des avis BSD.
01 juin 2004 ajout des références aux bulletins de sécurité GLSA-200405-13 et GLSA200405-25 de Gentoo.
08 juin 2004 ajout de la référence au bulletin de sécurité GLSA-200406-03 de Gentoo.
09 juin 2004 ajout de la référence au bulletin de sécurité de SUSE.
30 juillet 2004 ajout de la référence au bulletin de sécurité de Mandrake.