



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-135-007

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Neon

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-2004-AVI-135>

Gestion du document

Référence	CERTA-2004-AVI-135-007
Titre	Vulnérabilité de Neon
Date de la première version	20 avril 2004
Date de la dernière version	30 juillet 2004
Source(s)	Liste de diffusion BugTraq
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

Neon versions antérieures à la version 0.24.5.

3 Résumé

Plusieurs vulnérabilités de type `format string` ont été découvertes dans Neon qui permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Neon est une bibliothèque cliente WebDAV utilisée par un grand nombre d'applications WebDAV comme `subversion`, `cadaver`, `sitecopy` et `OpenOffice`.

Plusieurs vulnérabilités de type `format string` sont présentes dans le code de cette bibliothèque.

5 Solution

Mettre à jour votre version de Neon (cf. section documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-487 du 16 avril 2004 :
<http://www.debian.org/security/2004/dsa-487>
- Bulletin de sécurité Gentoo GLSA-200404-14 du 19 avril 2004 pour cadaver :
<http://www.gentoo.org/security/en/glsa/glsa-200404-14.xml>
- Bulletin de sécurité Gentoo GLSA-200405-01 du 09 mai 2004 pour neon :
<http://www.gentoo.org/security/en/glsa/glsa-200405-01.xml>
- Bulletin de sécurité Gentoo GLSA-200405-04 du 11 mai 2004 pour OpenOffice :
<http://www.gentoo.org/security/en/glsa/glsa-200405-04.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:032 du 19 avril 2004 pour libneon :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:032>
- Bulletin de sécurité Mandrake MDKSA-2004:078 du 29 juillet 2004 pour OpenOffice :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:078>
- Bulletin de sécurité Red Hat RHSA:2004-157 du 14 avril 2004 pour cadaver :
<http://rhn.redhat.com/errata/RHSA-2004-157.html>
- Bulletin de sécurité Red Hat RHSA:2004-158 du 14 avril 2004 pour cadaver :
<http://rhn.redhat.com/errata/RHSA-2004-158.html>
- Bulletin de sécurité Red Hat RHSA:2004-159 du 15 avril 2004 pour Subversion :
<http://rhn.redhat.com/errata/RHSA-2004-159.html>
- Bulletin de sécurité Red Hat RHSA:2004-160 du 14 avril 2004 pour OpenOffice :
<http://rhn.redhat.com/errata/RHSA-2004-160.html>
- Bulletin de sécurité Red Hat RHSA:2004-163 du 14 avril 2004 pour OpenOffice :
<http://rhn.redhat.com/errata/RHSA-2004-163.html>
- Bulletin de sécurité SUSE SuSE-SA:2004:008 du 14 avril 2004 :
http://www.suse.com/de/security/2004_08_cvs.html
- Bulletin de sécurité SUSE SuSE-SA:2004:015 du 09 juin 2004 pour sitecopy, cadaver, tla et OpenOffice :
http://www.suse.com/de/security/2004_15_cvs.html
- Bulletin de sécurité SGI 20040404-01-U du 21 avril 2004 :
<ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc>
- Bulletin de sécurité FreeBSD du 15 avril 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité pour le paquetage OpenBSD neon du 16 avril 2004 :
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité pour le paquetage OpenBSD cadaver du 14 avril 2004 :
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité du paquetage NetBSD neon :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2004-0179 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0179>

Gestion détaillée du document

20 avril 2004 version initiale.

3 mai 2004 ajout de la référence au bulletin de sécurité RedHat RHSA:2004-163 pour OpenOffice.

10 mai 2004 ajout des références aux bulletins de sécurité RedHat, SUSE et SGI, correction de la référence Debian.

11 mai 2004 ajout de la référence au bulletin de sécurité GLSA 200405-01 de Gentoo.

11 mai 2004 ajout de la référence au bulletin de sécurité GLSA 200405-04 de Gentoo pour OpenOffice.

12 mai 2004 ajout des références aux bulletins de sécurité FreeBSD, OpenBSD et NetBSD.

09 juin 2004 ajout des références aux bulletins de sécurité SUSE et RedHat.

30 juillet 2004 ajout de la référence au bulletin de sécurité Mandrake MDKSA-2004:078.