

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'OpenSSL

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-095>

Gestion du document

Référence	CERTA-2004-AVI-095-005
Titre	Multiples vulnérabilités d'OpenSSL
Date de la première version	18 mars 2004
Date de la dernière version	07 mai 2004
Source(s)	Bulletin de sécurité 224012 du NISCC Bulletin de sécurité d'OpenSSL du 17 mars 2004
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.

2 Systèmes affectés

Tout système se basant sur OpenSSL pour mettre en oeuvre les protocoles de session SSL et TLS.

Se référer aux différents bulletins de sécurité (cf. section Solution) pour obtenir la liste des systèmes vulnérables.

3 Résumé

A l'aide de trames habilement constituées, un utilisateur mal intentionné peut réaliser un déni de service par arrêt brutal d'un service réseau vulnérable.

4 Description

Deux vulnérabilités ont été découvertes dans le code gérant la phase d'établissement des sessions SSL/TLS.

A l'aide de trames habilement constituées, un utilisateur mal intentionné peut exploiter ces vulnérabilités afin de provoquer l'arrêt brutal d'un service réseau vulnérable.

Un correctif de sécurité ajouté à la version 0.9.6d d'OpenSSL a introduit une troisième vulnérabilité (référence CAN-2004-0081).

L'exploitation de cette vulnérabilité entraîne un déni de service par consommation excessive des ressources de la machine.

5 Solution

- Les versions 0.9.7d et 0.9.6m d'OpenSSL corrigent ces vulnérabilités :
<http://www.openssl.org>
- Bulletin de sécurité RHTSA-2004:120 de Red Hat :
<http://rhn.redhat.com/errata/RHTSA-2004-120.html>
- Bulletin de sécurité RHTSA-2004:121 de Red Hat :
<http://rhn.redhat.com/errata/RHTSA-2004-121.html>
- Bulletin de sécurité RHTSA-2004:139 de Red Hat :
<http://rhn.redhat.com/errata/RHTSA-2004-139.html>
- Bulletin de sécurité DSA-465 de Debian :
<http://www.debian.org/security/2004/dsa-465>
- Bulletin de sécurité MDKSA-2004:023 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:023>
- Bulletin de sécurité SuSE-SA:2004:007 de SuSE :
http://www.suse.com/de/security/2004_07_openssl.html
- Bulletin de sécurité GLSA 200403-03 de Gentoo :
<http://www.securityfocus.com/advisories/6460>
- Bulletin de sécurité #57524 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57524>
- Bulletin de sécurité FreeBSD-SA-04:05 de FreeBSD :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:05.openssl.asc>
- Correctif pour OpenBSD du 17 mars 2004 :
<http://www.openbsd.org/errata.html#openssl>
- Bulletin de sécurité "Cisco OpenSSL implementation vulnerability" de Cisco :
<http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml>
- Bulletin de sécurité #58466 de NetScreen :
<http://www.netscreen.com/services/security/alerts/adv58466-signed.txt>
- Bulletin de sécurité "OpenSSL Vulnerability" de Check Point :
<http://www.checkpoint.com/techsupport/alerts/openssl.html>
- Bulletin de sécurité NetBSD NetBSD-SA2004-005 :
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-005.txt.asc>
- Bulletin de sécurité HPSBUX01019 pour HP-UX :
<http://www.securityfocus.com/advisories/6623>
- Bulletin de sécurité HPSBMA01037 pour les agents de supervision HP WBEM :
<http://www.securityfocus.com/advisories/6674>
- Mise à jour de sécurité MacOS X :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-111/index.html>

6 Documentation

- Bulletin de sécurité 224012 du NISCC :
<http://www.uniras.gov.uk/vuls/2004/224012>
- Bulletin de sécurité d'OpenSSL du 17 mars 2004 :
http://www.openssl.org/news/secadv_20040317.txt

- Référence CVE CAN-2004-0079 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0079>
- Référence CVE CAN-2004-0112 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0112>
- Référence CVE CAN-2004-0081 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0081>

Gestion détaillée du document

18 mars 2004 version initiale.

22 mars 2004 ajout référence au bulletin de sécurité de NetScreen.

30 mars 2004 ajout référence au bulletin de sécurité de Check Point.

22 avril 2004 ajout référence au bulletin de sécurité de NetBSD.

27 avril 2004 ajout référence au bulletin de sécurité de Hewlett-Packard.

07 mai 2004 ajout références au bulletin de sécurité de Hewlett-Packard pour les agents de supervision HP WEBM et à l'avis du CERTA relatif au correctif de sécurité MacOS X.