



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 novembre 2007
N° CERTA-2007-AVI-423-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2007-AVI-423>

Gestion du document

Référence	CERTA-2007-AVI-423-002
Titre	Vulnérabilités d'OpenSSL
Date de la première version	04 octobre 2007
Date de la dernière version	30 novembre 2007
Source(s)	Bulletin Ubuntu USN-522-1 du 29 septembre 2007
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

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

OpenSSL, versions 0.9.8d et précédentes.

3 Résumé

Deux vulnérabilités affectent OpenSSL. La première permet à un utilisateur malveillant d'accéder à des données sensibles. La seconde permettrait à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une erreur entache l'implantation de l'algorithme de multiplication avec réduction modulaire de Montgomery. Cette erreur permet à un utilisateur malveillant de reconstruire la clé secrète utilisée.

Un défaut de vérification de taille de tampon mémoire existe dans la fonction *SSL_get_shared_ciphers*. Cette vulnérabilité permet à un utilisateur malveillant de provoquer un déni de service et lui permettrait d'exécuter du code arbitraire à distance.

5 Solution

La version 0.9.8-stable corrige ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Correctif OpenSSL du 29 juin 2007 :
<http://openssl.org/news/patch-CVE-2007-3108.txt>
- Bulletin OpenSSL du 19 septembre 2007 :
<http://cvs.openssl.org/chngview?cn=16587>
- Bulletin de sécurité Red Hat RHSA-2007:0964 du 12 octobre 2007 :
<https://rhn.redhat.com/errata/RHSA-2007:0964.html>
- Bulletin de sécurité OpenBSD ID 17 du 10 octobre 2007 :
<http://www.openbsd.org/errata40.html>
- Bulletin de sécurité Gentoo GLSA-200710-06 du 07 octobre 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200710-06.xml>
- Bulletin de sécurité Mandriva MDKSA-2007:193 du 04 octobre 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:193>
- Bulletin de sécurité SuSE SUSE-SR:2007:020 du 12 octobre 2007 :
http://www.novell.com/linux/security/advisories/2007_20_sr.html
- Bulletin de sécurité Ubuntu USN-522-1 du 29 septembre 2007 :
<http://www.ubuntulinux.org/usn/usn-522-1>
- Bulletin de sécurité Debian DSA-1379-1 du 02 octobre 2007 :
<http://www.debian.org/security/2007/dsa-1379>
- Bulletin de sécurité FreeBSD SA-07:08 du 03 octobre 2007 :
<http://security.freebsd.org/advisories/FreeBSD-SA-07:08.openssl.asc>
- Bulletin de sécurité Blue Coat du 27 novembre 2007 :
http://www.bluecoat.com/support/securityadvisories/advisory_openssl_rsa_key_reconstruction_vulnerability

- Référence CVE CVE-2007-3108 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3108>
- Référence CVE CVE-2007-4995 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4995> 5B
- Référence CVE CVE-2007-5135 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5135>

Gestion détaillée du document

04 octobre 2007 version initiale.

17 octobre 2007 ajout de la référence CVE-2007-4995 et des références aux bulletins de sécurité OpenBSD, Gentoo, Red Hat, SuSE et Mandriva.

30 novembre ajout de la référence Blue Coat.