CVE-2008-1672

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2008-1672
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-29 16:32:00 UTC
Updated	2022-02-02 15:03:00 UTC
Description	OpenSSL 0.9.8f and 0.9.8g allows remote attackers to cause a denial of service (crash) via a TLS handshake that omits the

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl Project	Openssl	0.9.8f	All	All	All
Application	Openssl Project	Openssl	0.9.8g	All	All	All
Application	Openssl Project	Openssl	0.9.8f	All	All	All
Application	Openssl Project	Openssl	0.9.8g	All	All	All

References

Reference	Source
[SECURITY] Fedora 9 Update: openssl-0.9.8g-9.fc9	FEDORA
OpenSSL: Denial of Service — Gentoo Linux Documentation	GENTOO
OpenSSL Multiple Denial of Service Vulnerabilities	BID
OpenSSL Two Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
CERT-FI - CERT-FI Vulnerability Advisory on OpenSSL	MISC
Nortel Media Processing Server OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA

The Slackware Linux Project: Slackware Security Advisories	SLACKWA
www.openssl.org/news/secadv_20080528.txt	CONFIRM
US-CERT Vulnerability Note VU#520586	CERT-VN
Webmail - OVH	VUPEN
SecurityFocus	BUGTRAC
Support / Security / Advisories / / MDVSA-2008:107 | Mandriva	MANDRIV
Ubuntu update for openssl - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
OpenSSL TLS Handshake Bug Lets Remote Servers Crash the Connected Client - SecurityTracker	SECTRAC
Gentoo update for openssl - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Fedora update for openssl - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
cwRsync OpenSSL Denial of Service Vulnerabilities - Advisories - Secunia	SECUNIA
Webmail - OVH	VUPEN
support.nortel.com/go/main.jsp	MISC
Slackware update for openssl - Advisories - Secunia	SECUNIA
SourceForge.net: SysAdmin Tools from ITeF!x: Files	CONFIRM
USN-620-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-05-30	Mark J Cox	Not vulnerable. This issue did not affect the versions of OpenSSL as shipped with Red Hat Ente

Legacy QID Mappings

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)