CVE-2007-4995

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-4995
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-13 01:17:00 UTC
Updated	2018-10-15 21:39:00 UTC
Description	Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary c

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All

References

Reference	Sour
HPSBUX02296	HP
USN-534-1: OpenSSL vulnerability | Ubuntu security notices	UBU

[security-announce] SUSE Security Summary Report SUSE-SR:2007:021	SUSE
Webmail - OVH	VUPE
Debian -- Security Information -- DSA-1571-1 openssl	DEBI
Mandriva update for openssl - Advisories - Secunia	SECU
SecurityTracker.com Archives - OpenSSL DTLS Bug May Let Remote Users Execute Arbitrary Code	SECT
OpenSSL DTLS Implementation Vulnerability - Advisories - Secunia	SECU
Gentoo Linux Documentation -- OpenSSL: Remote execution of arbitrary code	GENT
Nortel Media Processing Server OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECU
Ubuntu update for OpenSSL - Advisories - Secunia	SECU
www.openssl.org/news/secadv_20071012.txt	CONF
SecurityFocus	BUGT
IBM X-Force Exchange	XF
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation	GENT
SUSE Updates for Multiple Packages - Advisories - Secunia	SECU
Nortel: Technical Support: Nortel Response to OpenSSL DTLS Heap Buffer Overflow Vulnerability	MISC
Webmail - OVH	VUPE
Gentoo update for openssl - Advisories - Secunia	SECU
Repository / Oval Repository	OVAL
Red Hat update for openssl - Advisories - Secunia	SECU
HP-UX update for OpenSSL - Advisories - Secunia	SECU
OpenSSL DTLS Heap Buffer Overflow Vulnerability	BID
rhn.redhat.com | Red Hat Support	REDH
Webmail - OVH	VUPE
Gentoo ltsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECU
Support / Security / Advisories / / MDKSA-2007:237 | Mandriva	MAND
Debian OpenSSL Predictable Random Number Generator and Update - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
Fedora update for openssl - Advisories - Secunia	SECU
[SECURITY] Fedora Core 6 Update: openssl-0.9.8b-15.fc6	FEDO
Gentoo Bug 195634 - dev-libs/openssl < 0.9.8f DTLS vulnerability (CVE-2007-4995)	CONF
CVE Program record	CVE.(
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-10-24	Mark J Cox	This issue did not affect the versions of OpenSSL as shipped with Red Hat Enterprise Linux 2.1,

Legacy QID Mappings

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