CVE-2008-0166

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2008-0166
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-13 17:20:00 UTC
Updated	2022-02-02 14:59:00 UTC
Description	OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator th

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Openssl	Openssl	0.9.8c-1	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl Project	Openssl	0.9.8c-1	All	All	All
Application	Openssl Project	Openssl	0.9.8c-2	All	All	All
Application	Openssl Project	Openssl	0.9.8c-3	All	All	All
Application	Openssl Project	Openssl	0.9.8c-4	All	All	All
Application	Openssl Project	Openssl	0.9.8c-5	All	All	All
Application	Openssl Project	Openssl	0.9.8c-6	All	All	All
Application	Openssl Project	Openssl	0.9.8c-7	All	All	All
Application	Openssl Project	Openssl	0.9.8c-8	All	All	All

Application	Openssl Project	Openssl	0.9.8c-9	All	All	All
Application	Openssl Project	Openssl	0.9.8d-1	All	All	All
Application	Openssl Project	Openssl	0.9.8d-2	All	All	All
Application	Openssl Project	Openssl	0.9.8d-3	All	All	All
Application	Openssl Project	Openssl	0.9.8d-4	All	All	All
Application	Openssl Project	Openssl	0.9.8d-5	All	All	All
Application	Openssl Project	Openssl	0.9.8d-6	All	All	All
Application	Openssl Project	Openssl	0.9.8d-7	All	All	All
Application	Openssl Project	Openssl	0.9.8d-8	All	All	All
Application	Openssl Project	Openssl	0.9.8d-9	All	All	All
Application	Openssl Project	Openssl	0.9.8e-1	All	All	All
Application	Openssl Project	Openssl	0.9.8e-2	All	All	All
Application	Openssl Project	Openssl	0.9.8e-3	All	All	All
Application	Openssl Project	Openssl	0.9.8e-4	All	All	All
Application	Openssl Project	Openssl	0.9.8e-5	All	All	All
Application	Openssl Project	Openssl	0.9.8e-6	All	All	All
Application	Openssl Project	Openssl	0.9.8e-7	All	All	All
Application	Openssl Project	Openssl	0.9.8e-8	All	All	All
Application	Openssl Project	Openssl	0.9.8e-9	All	All	All
Application	Openssl Project	Openssl	0.9.8f-1	All	All	All
Application	Openssl Project	Openssl	0.9.8f-2	All	All	All
Application	Openssl Project	Openssl	0.9.8f-3	All	All	All
Application	Openssl Project	Openssl	0.9.8f-4	All	All	All
Application	Openssl Project	Openssl	0.9.8f-5	All	All	All
Application	Openssl Project	Openssl	0.9.8f-6	All	All	All
Application	Openssl Project	Openssl	0.9.8f-7	All	All	All
Application	Openssl Project	Openssl	0.9.8f-8	All	All	All
Application	Openssl Project	Openssl	0.9.8f-9	All	All	All
Application	Openssl Project	Openssl	0.9.8g-1	All	All	All
Application	Openssl Project	Openssl	0.9.8g-2	All	All	All
Application	Openssl Project	Openssl	0.9.8g-3	All	All	All
Application	Openssl Project	Openssl	0.9.8g-4	All	All	All
Application	Openssl Project	Openssl	0.9.8g-5	All	All	All
Application	Openssl Project	Openssl	0.9.8g-6	All	All	All
Application	Openssl Project	Openssl	0.9.8g-7	All	All	All

Application	Openssl Project	Openssl	0.9.8g-8	All	All	All
Application	Openssl Project	Openssl	0.9.8g-9	All	All	All
Application	Openssl Project	Openssl	0.9.8c-1	All	All	All
Application	Openssl Project	Openssl	0.9.8c-2	All	All	All
Application	Openssl Project	Openssl	0.9.8c-3	All	All	All
Application	Openssl Project	Openssl	0.9.8c-4	All	All	All
Application	Openssl Project	Openssl	0.9.8c-5	All	All	All
Application	Openssl Project	Openssl	0.9.8c-6	All	All	All
Application	Openssl Project	Openssl	0.9.8c-7	All	All	All
Application	Openssl Project	Openssl	0.9.8c-8	All	All	All
Application	Openssl Project	Openssl	0.9.8c-9	All	All	All
Application	Openssl Project	Openssl	0.9.8d-1	All	All	All
Application	Openssl Project	Openssl	0.9.8d-2	All	All	All
Application	Openssl Project	Openssl	0.9.8d-3	All	All	All
Application	Openssl Project	Openssl	0.9.8d-4	All	All	All
Application	Openssl Project	Openssl	0.9.8d-5	All	All	All
Application	Openssl Project	Openssl	0.9.8d-6	All	All	All
Application	Openssl Project	Openssl	0.9.8d-7	All	All	All
Application	Openssl Project	Openssl	0.9.8d-8	All	All	All
Application	Openssl Project	Openssl	0.9.8d-9	All	All	All
Application	Openssl Project	Openssl	0.9.8e-1	All	All	All
Application	Openssl Project	Openssl	0.9.8e-2	All	All	All
Application	Openssl Project	Openssl	0.9.8e-3	All	All	All
Application	Openssl Project	Openssl	0.9.8e-4	All	All	All
Application	Openssl Project	Openssl	0.9.8e-5	All	All	All
Application	Openssl Project	Openssl	0.9.8e-6	All	All	All
Application	Openssl Project	Openssl	0.9.8e-7	All	All	All
Application	Openssl Project	Openssl	0.9.8e-8	All	All	All
Application	Openssl Project	Openssl	0.9.8e-9	All	All	All
Application	Openssl Project	Openssl	0.9.8f-1	All	All	All
Application	Openssl Project	Openssl	0.9.8f-2	All	All	All
Application	Openssl Project	Openssl	0.9.8f-3	All	All	All
Application	Openssl Project	Openssl	0.9.8f-4	All	All	All
Application	Openssl Project	Openssl	0.9.8f-5	All	All	All
Application	Openssl Project	Openssl	0.9.8f-6	All	All	All

Application	Openssl Project	Openssl	0.9.8f-7	All	All	All
Application	Openssl Project	Openssl	0.9.8f-8	All	All	All
Application	Openssl Project	Openssl	0.9.8f-9	All	All	All
Application	Openssl Project	Openssl	0.9.8g-1	All	All	All
Application	Openssl Project	Openssl	0.9.8g-2	All	All	All
Application	Openssl Project	Openssl	0.9.8g-3	All	All	All
Application	Openssl Project	Openssl	0.9.8g-4	All	All	All
Application	Openssl Project	Openssl	0.9.8g-5	All	All	All
Application	Openssl Project	Openssl	0.9.8g-6	All	All	All
Application	Openssl Project	Openssl	0.9.8g-7	All	All	All
Application	Openssl Project	Openssl	0.9.8g-8	All	All	All
Application	Openssl Project	Openssl	0.9.8g-9	All	All	All

References

Reference	Sour
Ubuntu update for openvpn - Advisories - Secunia	SECU
US-CERT Technical Cyber Security Alert TA08-137A -- Debian/Ubuntu OpenSSL Random Number Generator Vulnerability	CERT
USN-612-4: ssl-cert vulnerability | Ubuntu	UBUN
USN-612-7: OpenSSH update | Ubuntu	UBUN
Debian OpenSSL Predictable PRNG Bruteforce SSH Exploit (Python)	EXPL
Ubuntu update for ssl-cert - Advisories - Secunia	SECU
Debian -- Security Information -- DSA-1571-1 openssl	DEBI
USN-612-1: OpenSSL vulnerability | Ubuntu	UBUN
Debian OpenSSL Predictable PRNG Bruteforce SSH Exploit (ruby)	EXPL
US-CERT Vulnerability Note VU#925211	CERT
Debian OpenSSL Package Random Number Generator Weakness	BID
USN-612-2: OpenSSH vulnerability | Ubuntu	UBUN
USN-612-3: OpenVPN vulnerability | Ubuntu	UBUN
IBM X-Force Exchange	XF
Debian -- Security Information -- DSA-1576-1 openssh	DEBI
SourceForge.net: rsync friendly file encryption: rsyncrypto-devel	MLIS
Ubuntu update for openssl - Advisories - Secunia	SECU
Debian update for openssh - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
SecurityTracker.com Archives - OpenSSL for Debian/Ubuntu Predictable RNG Lets Remote Users Determine Cryptographic Keys	SECT
SecurityFocus	BUGT
Debian OpenSSL Predictable PRNG Toys	MISC

Debian OpenSSL Predictable PRNG Bruteforce SSH Exploit	EXPL
Debian OpenSSL Predictable Random Number Generator and Update - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
Ubuntu update for openssh - Advisories - Secunia	SECU
CVE Program record	CVE.(
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-05-13	Mark J Cox	Not vulnerable. This flaw was caused by a third-party vendor patch to the OpenSSL library. This

There are currently no legacy QID mappings associated with this CVE.