CVE-2009-0789

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0789
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-27 16:30:02 UTC
Updated	2026-04-23 00:35:47 UTC
Description	OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, whic

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.1c	All	All	All

Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All

Application	Openssl	Openssl	0.9.7	beta6	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All
Application	Openssl	Openssl	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	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
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
SUSE Update for Multiple Packages - Advisories - Community	af854a3a-212
www.openssl.org/news/secadv_20090325.txt	af854a3a-212
kb.bluecoat.com/index	af854a3a-212
About Secunia Research | Flexera	af854a3a-212

NetBSD update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
Webmail - OVH	af854a3a-212
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:010	af854a3a-212
'[security bulletin] HPSBOV02540 SSRT090249 rev.1 - HP SSL for OpenVMS, Remote Unauthorized Data Inje' - MARC	af854a3a-212
Webmail - OVH	af854a3a-212
PHP: News Archive - 2009	af854a3a-212
ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2009-008.txt.asc	af854a3a-212
[security-announce] openSUSE-SU-2011:0845-1: important: compat-openssl09	af854a3a-212
OpenSSL Multiple Vulnerabilities	af854a3a-212
IBM X-Force Exchange	af854a3a-212
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
PHP for Windows OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
HP-UX update for OpenSSL - Secunia.com	af854a3a-212
VooDoo cIRCle download | SourceForge.net	af854a3a-212
VooDoo cIRCle OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
Webmail | OVH- OVH	af854a3a-212
About Secunia Research | Flexera	af854a3a-212
www.osvdb.org/52866	af854a3a-212
VooDoo cIRCle security advisory 20090326-01	af854a3a-212
OpenSSL ASN1 Structure Memory Access Error Lets Users Deny Service - SecurityTracker	af854a3a-212
marc.info	af854a3a-212
OpenSSL Multiple Vulnerabilities - Advisories - Community	af854a3a-212
About Security Update 2009-005	af854a3a-212
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-212
APPLE-SA-2009-09-10-2 Security Update 2009-005	af854a3a-212
[security-announce] SUSE-SU-2011:0847-1: important: Security update for	af854a3a-212
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-03-30	Tomas Hoger	Not vulnerable. This issue only affects a small number of operating systems and does not affec

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report