CVE-2003-0131

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

Summary

CVE	CVE-2003-0131
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-03-24 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The SSL and TLS components for OpenSSL 0.9.6i and earlier, 0.9.7, and 0.9.7a allow remote attackers to perform an unau

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.6	All	All	All

Application	Openssl	Openssl	0.9.6a	All	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	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
'TSLSA-2003-0013 - openssl' - MARC	af854a3a-2127-422
LinuxSecurity.com: Immunix: openssl, openssh, mod_ssl multiple vulnerabilities	af854a3a-2127-422
SuSE Security Announcement: openssl (SuSE-SA:2003:024)	af854a3a-2127-422
redhat.com | Red Hat Support	af854a3a-2127-422
ftp.sco.com/pub/security/OpenLinux/CSSA-2003-014.0.txt	af854a3a-2127-422
Apple - Lists.apple.com	af854a3a-2127-422
Gentoo Linux — Error 404 (Not Found)	af854a3a-2127-422
ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc	af854a3a-2127-422
patches.sgi.com/support/free/security/advisories/20030501-01-I	af854a3a-2127-422
redhat.com | Red Hat Support	af854a3a-2127-422
www.openssl.org/news/secadv_20030319.txt	af854a3a-2127-422
Repository / Oval Repository	af854a3a-2127-422
OpenPKG: Security Advisory [OpenPKG-SA-2003.026-openssl]	af854a3a-2127-422
'[OpenSSL Advisory] Klima-Pokorny-Rosa attack on PKCS #1 v1.5 padding' - MARC	af854a3a-2127-422
Mandriva Security Advisories	af854a3a-2127-422
eprint.iacr.org/2003/052	af854a3a-2127-422
'GLSA: openssl (200303-20)' - MARC	af854a3a-2127-422
Home - Conectiva	af854a3a-2127-422
OpenSSL Bad Version Oracle Side Channel Attack Vulnerability	af854a3a-2127-422
SecurityFocus	af854a3a-2127-422

SecurityFocus	af854a3a-2127-422
IBM X-Force Exchange	af854a3a-2127-422
VU#888801 - SSL/TLS implementations disclose side channel information via PKCS #1 v1.5 version number extension	af854a3a-2127-422
Debian -- Security Information -- DSA-288-1 openssl	af854a3a-2127-422
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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