CVE-2003-0544

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

Summary

CVE	CVE-2003-0544
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-11-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	OpenSSL 0.9.6 and 0.9.7 does not properly track the number of characters in certain ASN.1 inputs, which allows remote at

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: NVD-CWE-Other | 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	0.9.6	All	All	All

Application	Openssl	Openssl	0.9.7	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-2127-422b-91
CERT/CC Vulnerability Note VU#380864	af854a3a-2127-422b-91
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-393-1 openssl	af854a3a-2127-422b-91
Repository / Oval Repository	af854a3a-2127-422b-91
LinuxSecurity.com: EnGarde: OpenSSL ASN.1 parsing vulnerabilities	af854a3a-2127-422b-91
Bug 104893 - CAN-2003-0543/0544 OpenSSL ASN.1 protocol crashes	af854a3a-2127-422b-91
redhat.com | Red Hat Support	af854a3a-2127-422b-91
OpenSSL ASN.1 Parsing Vulnerabilities	af854a3a-2127-422b-91
IBM Vulnerability Detected: 170.23.146.40:443 - OpenSSL Overflow Via Invalid Certificate Passing - United States	af854a3a-2127-422b-91
Webmail - OVH	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-394-1 openssl095	af854a3a-2127-422b-91
IBM Rational RequisitePro OpenSSL Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91
www.uniras.gov.uk/vuls/2003/006489/openssl.htm	af854a3a-2127-422b-91
sunsolve.sun.com/search/document.do	af854a3a-2127-422b-91
CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations	af854a3a-2127-422b-91
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-07-07	Mark J Cox	For Red Hat Enterprise Linux 2.1 OpenSSL packages (openssl, openssl096, openssl095a) issue

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