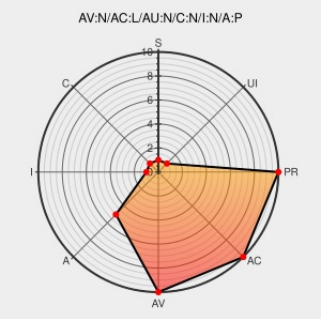
CVE-2003-0543

Published on: 10/01/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-0543

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssl from Openssl contain the following vulnerability:

Integer overflow in OpenSSL 0.9.6 and 0.9.7 allows remote attackers to cause a denial of service (crash) via an SSL client certificate with certain ASN.1 tag values.

CVE-2003-0543 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4254
Bug 104893 - CAN-2003-0543/0544 OpenSSL ASN.1 protocol crashes	Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=104893
CERT/CC Vulnerability Note VU#255484	US Government Resource www.kb.cert.org text/html	CERT-VN VU#255484
LinuxSecurity.com: EnGarde: OpenSSL ASN.1 parsing vulnerabilities	www.linuxsecurity.com text/html	ENGARDE ESA-20030930-027
IBM Rational RequisitePro OpenSSL Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 22249

OpenSSL ASN.1 Parsing Vulnerabilities	cve.report (archive) text/html	BID 8732
IBM Vulnerability Detected: 170.23.146.40:443 - OpenSSL Overflow Via Invalid Certificate Passing - United States	web.archive.org text/html Inactive Link Not Archived	CONFIRM www-1.ibm.com/support/docview.wss?uid=swg21247112
redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2003:291
No Description Provided	sunsolve.sun.com Inactive Link Not Archived	SUNALERT 201029
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-3900
Debian -- Security Information -- DSA-393-1 openssl	www.debian.org Depreciated Link text/html	DEBIAN DSA-393
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:5292
Debian -- Security Information -- DSA-394-1 openssl095	www.debian.org Depreciated Link text/html	DEBIAN DSA-394
CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations	US Government Resource www.cert.org text/html	CERT CA-2003-26
No Description Provided	web.archive.org text/html Inactive Link Not Archived	MISC www.uniras.gov.uk/vuls/2003/006489/openssl.htm
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:292

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All

cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:*:*:

← Previous ID

Next ID→