CVE-2002-1568

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

Summary

CVE	CVE-2002-1568
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 0.9.6e uses assertions when detecting buffer overflow attacks instead of less severe mechanisms, which allows r

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	0.9.6e	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
www.ebitech.sk/patrik/SA/SA-20031002.txt	af854a3a-2127-422b-91ae-364da2661108	www.ebitech.sk	
'New OpenSSL remote vulnerability (issue date 2003/10/02)' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
cvs.openssl.org/chngview	af854a3a-2127-422b-91ae-364da2661108	cvs.openssl.org	Patch,
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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