



CVE-2004-0004

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2004-0004
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-02-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The libCheckSignature function in crypto-utils.lib for OpenCA 0.9.1.6 and earlier only compares the serial of the signer's cer

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	Openca	Openca	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		Link	
'[OpenCA Advisory] Vulnerability in signature verification' - MARC	af854a3a-2127-422b-91ae-364da2661108		marc.info	
US-CERT Vulnerability Note VU#336446	af854a3a-2127-422b-91ae-364da2661108		www.kb.cert.org	
404 Not Found	af854a3a-2127-422b-91ae-364da2661108		www.openca.org	
www.osvdb.org/3615	af854a3a-2127-422b-91ae-364da2661108		www.osvdb.org	
OpenCA Crypto-Utils.Lib Signature Verification Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com	
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108		exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG		www.cve.org	
NVD vulnerability detail	NVD		nvd.nist.gov	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				