CVE-2007-2466

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

Summary

CVE	CVE-2007-2466
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-02 22:19:00 UTC
Updated	2017-07-29 01:31:00 UTC
Description	Unspecified vulnerability in the LDAP Software Development Kit (SDK) for C, as used in Sun Java System Directory Server

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sun	Java System Directory Server	5.2	All	All	All
Application	Sun	Java System Directory Server	5.2	2003q4	All	All
Application	Sun	Java System Directory Server	5.2	2004q2	All	All
Application	Sun	Java System Directory Server	5.2	2005q1	All	All
Application	Sun	Java System Directory Server	5.2	2005q4	All	All
Application	Sun	Java System Directory Server	5.2	All	All	All
Application	Sun	Java System Directory Server	5.2	2003q4	All	All
Application	Sun	Java System Directory Server	5.2	2004q2	All	All
Application	Sun	Java System Directory Server	5.2	2005q1	All	All
Application	Sun	Java System Directory Server	5.2	2005q4	All	All
Application	Sun	One Directory Server	5.1	All	All	All
Application	Sun	One Directory Server	5.1	All	All	All

References

Reference	Source	Li
Sun Java System Directory Server Denial of Service - Advisories - Secunia	SECUNIA	se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww

Sun Java System Directory Server BER Decoding Denial Of Service Vulnerability	BID	w
35743	OSVDB	os
SecurityTracker.com Archives - Sun Java System Directory Server BER Decoding Flaw Lets Remote Users Deny Service	SECTRACK	w
IBM X-Force Exchange	XF	ex
#201066: Security Vulnerability in Sun Java System Directory Server May Cause Denial of Service (DoS)	SUNALERT	su
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**