



CVE-2009-2240

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

Summary

CVE	CVE-2009-2240
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-27 18:48:00 UTC
Updated	2009-06-30 04:00:00 UTC
Description	Cross-site scripting (XSS) vulnerability in AD2000 free-sw leger (aka Web Conference Room Free) 1.6.4 and earlier allows

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ad2000	Free-sw Leger	All	All	All	All

References

Reference	Source	Link
JVN#57036470 Cross-site scripting vulnerability in leger (free edition)	JVN	jvn
WEB会議室予約 free-sw l e g e r	CONFIRM	v
JVNDB-2009-000031	JVNDB	jvn
Web Conference Room Free Cross-Site Scripting Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	s
Web Conference Room Free Unspecified Cross Site Scripting Vulnerability	BID	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)