CVE-2014-5114

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

Summary

CVE	CVE-2014-5114
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-29 14:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	WeBid 1.1.1 allows remote attackers to conduct an LDAP injection attack via the (1) js or (2) cat parameter.

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	Webidsupport	Webid	1.1.1	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
WeBid Multiple Cross Site Scripting And LDAP Injection Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
WeBid 1.1.1 Cross Site Scripting / LDAP Injection ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packetstormsecurity.co
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.