CVE-2006-1001

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

Summary

CVE	CVE-2006-1001
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-06 20:06:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	SQL injection vulnerability in the board module in LanSuite LanParty Intranet System 2.0.6 and 2.1.0 beta allows remote att

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:N

EPSS: 0.020420000 probability, percentile 0.838680000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Lansuite	Lanparty Intranet System	2.0.6	All	All	All
Application	Lansuite	Lanparty Intranet System	2.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-2127-422b-9
www.osvdb.org/23533	af854a3a-2127-422b-9
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-9
Lansuite Board Module SQL Injection Vulnerability	af854a3a-2127-422b-9
LanSuite LanParty Intranet System "fid" SQL Injection - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-9
Lansuite <= 2.1.0 Beta (fid) Remote SQL Injection Exploit	af854a3a-2127-422b-9
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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