CVE-2001-0440

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

Summary

CVE	CVE-2001-0440
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in logging functions of licq before 1.0.3 allows remote attackers to cause a denial of service, and possibly ex

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
Operating System	Conectiva	Linux	4.0	All	All	All

Operating System	Conectiva	Linux	4.0es	All	All	All
Operating System	Conectiva	Linux	4.1	All	All	All
Operating System	Conectiva	Linux	4.2	All	All	All
Operating System	Conectiva	Linux	5.0	All	All	All
Operating System	Conectiva	Linux	5.1	All	All	All
Operating System	Conectiva	Linux	6.0	All	All	All
Operating System	Conectiva	Linux	ecommerce	All	All	All
Operating System	Conectiva	Linux	prg_graficos	All	All	All
Application	Licq	Licq	All	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	7.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	7.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sc
www.linux-mandrake.com/en/security/2001/MDKSA-2001-032.php3	af
redhat.com | Red Hat Support	af
redhat.com | Red Hat Support	af
Home - Conectiva	af
Neohapsis Archives - FreeBSD Security - FreeBSD Security Advisory FreeBSD-SA-01:35.licq - From security-advisories@FreeBSD.org	af
IBM X-Force Exchange	af
404 Not Found	af
CVE Program record	CV
NVD vulnerability detail	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**