CVE-2003-0826

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

Summary

CVE	CVE-2003-0826
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-10-06 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	lsh daemon (lshd) does not properly return from certain functions in (1) read_line.c, (2) channel_commands.c, or (3) client_

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	Gnu	Lsh	1.4	All	All	All

Application	Gnu	Lsh	1.4.1	All	All	All
Application	Gnu	Lsh	1.4.2	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
lsh patch (was Re: [Full-Disclosure] new ssh exploit?)	af854a3a-2127-422b-91ae-364da2661108	lists
#211662 - lsh-server: heap overrun, possible remote root exploit - Debian Bug report logs	af854a3a-2127-422b-91ae-364da2661108	bugs
'LSH: Buffer overrun and remote root compromise in lshd' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc
lshd buffer overrun. Possibly remote root compromise.	af854a3a-2127-422b-91ae-364da2661108	lists
'Remote root vuln in lsh 1.4.x' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc
Debian -- Security Information -- DSA-717-1 lsh-utils	af854a3a-2127-422b-91ae-364da2661108	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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