



CVE-2005-0814

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

Summary

CVE	CVE-2005-0814
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Unknown vulnerability in lshd in Lysator LSH 1.x and 2.x before 2.0.1 allows remote attackers to cause a denial of service via a crafted packet.

Risk And Classification

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

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lysator	Lsh	1.0	All	All	All

Application	Lysator	Lsh	1.0.1	All	All	All
Application	Lysator	Lsh	1.0.2	All	All	All
Application	Lysator	Lsh	1.0.3	All	All	All
Application	Lysator	Lsh	1.0.4	All	All	All
Application	Lysator	Lsh	1.0.5	All	All	All
Application	Lysator	Lsh	1.0.6	All	All	All
Application	Lysator	Lsh	1.0.7	All	All	All
Application	Lysator	Lsh	1.1.0	All	All	All
Application	Lysator	Lsh	1.1.1	All	All	All
Application	Lysator	Lsh	1.1.2	All	All	All
Application	Lysator	Lsh	1.1.3	All	All	All
Application	Lysator	Lsh	1.1.4	All	All	All
Application	Lysator	Lsh	1.1.5	All	All	All
Application	Lysator	Lsh	1.1.6	All	All	All
Application	Lysator	Lsh	1.1.7	All	All	All
Application	Lysator	Lsh	1.1.8	All	All	All
Application	Lysator	Lsh	1.1.9	All	All	All
Application	Lysator	Lsh	1.2	All	All	All
Application	Lysator	Lsh	1.2.1	All	All	All
Application	Lysator	Lsh	1.2.2	All	All	All
Application	Lysator	Lsh	1.2.3	All	All	All
Application	Lysator	Lsh	1.2.4	All	All	All
Application	Lysator	Lsh	1.2.5	All	All	All
Application	Lysator	Lsh	1.3.0	All	All	All
Application	Lysator	Lsh	1.3.1	All	All	All
Application	Lysator	Lsh	1.3.2	All	All	All
Application	Lysator	Lsh	1.3.3	All	All	All
Application	Lysator	Lsh	1.3.4	All	All	All
Application	Lysator	Lsh	1.3.5	All	All	All
Application	Lysator	Lsh	1.3.6	All	All	All
Application	Lysator	Lsh	1.3.7	All	All	All
Application	Lysator	Lsh	1.4	All	All	All
Application	Lysator	Lsh	1.4.1	All	All	All
Application	Lysator	Lsh	1.4.2	All	All	All
Application	Lysator	Lsh	1.4.3	All	All	All
Application	Lysator	Lsh	1.5	All	All	All

Application	Lysator	Lsh	1.5.1	All	All	All
Application	Lysator	Lsh	1.5.2	All	All	All
Application	Lysator	Lsh	1.5.3	All	All	All
Application	Lysator	Lsh	1.5.4	All	All	All
Application	Lysator	Lsh	1.5.5	All	All	All
Application	Lysator	Lsh	2.0	All	All	All
Application	Lysator	Lsh	2.0.1	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	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108		exchange.xforce.it	
Debian -- Security Information -- DSA-717-1 lsh-utils			af854a3a-2127-422b-91ae-364da2661108		www.debian.org	
ANNOUNCE: LSH-2.0.1, fix for denial of service bug			af854a3a-2127-422b-91ae-364da2661108		lists.lysator.liu.se	
Secunia - Advisories - LSH lshd Unspecified Denial of Service Vulnerability			af854a3a-2127-422b-91ae-364da2661108		secunia.com	
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.