



CVE-2003-0963

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

Summary

CVE	CVE-2003-0963
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-01-05 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflows in (1) try_netscape_proxy and (2) try_squid_eplf for lftp 2.6.9 and earlier allow remote HTTP servers to 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
Application	Alexander V. Lukyanov	Lftp	2.3	All	All	All

Application	Alexander V. Lukyanov	Lftp	2.4.9	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.5.2	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.0	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.3	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.4	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.5	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.6	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.7	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.8	All	All	All
Application	Alexander V. Lukyanov	Lftp	2.6.9	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	Ta	
redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com		
Advisories - Mandriva	af854a3a-2127-422b-91ae-364da2661108	www.mandriva.com		
Secunia - Advisories - Conectiva update for lftp	af854a3a-2127-422b-91ae-364da2661108	secunia.com		
marc.info	af854a3a-2127-422b-91ae-364da2661108	marc.info		
patches.sgi.com/support/free/security/advisories/20040101-01-U	af854a3a-2127-422b-91ae-364da2661108	patches.sgi.com		
Debian -- Security Information -- DSA-406-1 lftp	af854a3a-2127-422b-91ae-364da2661108	www.debian.org		
marc.info	af854a3a-2127-422b-91ae-364da2661108	marc.info		
patches.sgi.com/support/free/security/advisories/20040202-01-U.asc	af854a3a-2127-422b-91ae-364da2661108	patches.sgi.com		
marc.info	af854a3a-2127-422b-91ae-364da2661108	marc.info		
redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com		
'GLSA: lftp (200312-07)' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info		
'[slackware-security] lftp security update (SSA:2003-346-01)' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info		
Secunia - Advisories - Debian update for lftp	af854a3a-2127-422b-91ae-364da2661108	secunia.com		
NOVELL: Broken Link - 404 Error Pages	af854a3a-2127-422b-91ae-364da2661108	www.novell.com		
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org		
CVE Program record	CVE.ORG	www.cve.org	ca	
NVD vulnerability detail	NVD	nvd.nist.gov	ca	

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)