CVE-2004-0235

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

Summary

CVE	CVE-2004-0235
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple directory traversal vulnerabilities in LHA 1.14 allow remote attackers or local users to create arbitrary files via an LH

Risk And Classification

Primary CVSS: v2.0 6.4 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clearswift	Mailsweeper	4.0	All	All	All

Application	Clearswift	Mailsweeper	4.1	All	All	All
Application	Clearswift	Mailsweeper	4.2	All	All	All
Application	Clearswift	Mailsweeper	4.3	All	All	All
Application	Clearswift	Mailsweeper	4.3.10	All	All	All
Application	Clearswift	Mailsweeper	4.3.11	All	All	All
Application	Clearswift	Mailsweeper	4.3.13	All	All	All
Application	Clearswift	Mailsweeper	4.3.3	All	All	All
Application	Clearswift	Mailsweeper	4.3.4	All	All	All
Application	Clearswift	Mailsweeper	4.3.5	All	All	All
Application	Clearswift	Mailsweeper	4.3.6	All	All	All
Application	Clearswift	Mailsweeper	4.3.6_sp1	All	All	All
Application	Clearswift	Mailsweeper	4.3.7	All	All	All
Application	Clearswift	Mailsweeper	4.3.8	All	All	All
Application	F-secure	F-secure Anti-virus	2003	All	All	All
Application	F-secure	F-secure Anti-virus	2004	All	All	All
Application	F-secure	F-secure Anti-virus	4.51	All	linux_gateways	All
Application	F-secure	F-secure Anti-virus	4.51	All	linux_servers	All
Application	F-secure	F-secure Anti-virus	4.51	All	linux_workstations	All
Application	F-secure	F-secure Anti-virus	4.52	All	linux_gateways	All
Application	F-secure	F-secure Anti-virus	4.52	All	linux_servers	All
Application	F-secure	F-secure Anti-virus	4.52	All	linux_workstations	All
Application	F-secure	F-secure Anti-virus	4.60	All	samba_servers	All
Application	F-secure	F-secure Anti-virus	5.41	All	mimesweeper	All
Application	F-secure	F-secure Anti-virus	5.41	All	windows_servers	All
Application	F-secure	F-secure Anti-virus	5.41	All	workstations	All
Application	F-secure	F-secure Anti-virus	5.42	All	mimesweeper	All
Application	F-secure	F-secure Anti-virus	5.42	All	windows_servers	All
Application	F-secure	F-secure Anti-virus	5.42	All	workstations	All
Application	F-secure	F-secure Anti-virus	5.5	All	client_security	All
Application	F-secure	F-secure Anti-virus	5.52	All	client_security	All
Application	F-secure	F-secure Anti-virus	6.21	All	ms_exchange	All
Application	F-secure	F-secure For Firewalls	6.20	All	All	All
Application	F-secure	F-secure Internet Security	2003	All	All	All
Application	F-secure	F-secure Internet Security	2004	All	All	All
Application	F-secure	F-secure Personal Express	4.5	All	All	All
Application	F-secure	F-secure Personal Express	4.6	All	All	All

Application	F-secure	F-secure Personal Express	4.7	All	All	All
Application	F-secure	Internet Gatekeeper	6.31	All	All	All
Application	F-secure	Internet Gatekeeper	6.32	All	All	All
Application	Rarlab	Winrar	3.20	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Application	Redhat	Lha	1.14i-9	All	i386	All
Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	3.0	All	All	All
Application	Stalker	Cgpmcafee	3.2	All	All	All
Application	Tsugio Okamoto	Lha	1.14	All	All	All
Application	Tsugio Okamoto	Lha	1.15	All	All	All
Application	Tsugio Okamoto	Lha	1.17	All	All	All
Application	Winzip	Winzip	9.0	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
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org
'[Ulf Harnhammar]: LHA Advisory + Patch' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcl
Debian -- Security Information -- DSA-515-1 lha	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
[Full-Disclosure] LHa buffer overflows and directory traversal problems	af854a3a-2127-422b-91ae-364da2661108	lists.grok.org.uk
Home - Conectiva	af854a3a-2127-422b-91ae-364da2661108	distro.conectiva.com.br
bugzilla.fedora.us/show_bug.cgi	af854a3a-2127-422b-91ae-364da2661108	bugzilla.fedora.us
Gentoo Linux Documentation -- Multiple vulnerabilities in LHa	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org
Multiple LHA Buffer Overflow/Directory Traversal Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
redhat.com | Red Hat, Inc.	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org
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.

© 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 registred 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**