



CVE-2006-1044

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-1044
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-07 11:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in LISTSERV 14.3 and 14.4, including LISTSERV Lite and HPO, with the web archive interface en

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

EPSS: 0.251300000 probability, percentile 0.961890000 (date 2026-04-16)

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	Lsoft	Listserv	14.3	All	All	All
Application	Lsoft	Listserv	14.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
SecurityTracker.com Archives - LISTSERV Web Archive Interface Unspecified Bugs Let Remote Users Execute Arbitrary Code	af854a3a-2
L-Soft Listserv 14.3 and 14.4 Multiple Unspecified Vulnerabilities	af854a3a-2
SecurityFocus	af854a3a-2
www.lsoft.com/manuals/1.8e/relnotes/LISTSERV14.5-Release-Notes.html	af854a3a-2
Advisories - Research - Next Generation Security Software	af854a3a-2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2
US-CERT Vulnerability Note VU#841132	af854a3a-2
LISTSERV WA CGI Script Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2
IBM X-Force Exchange	af854a3a-2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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