



CVE-2004-2068

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

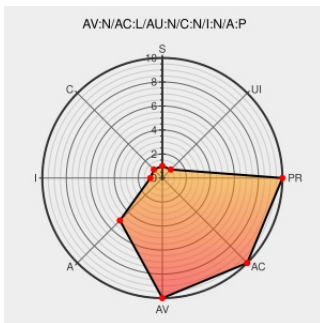
CVE-2004-2068

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Leafnode](#) from [Leafnode](#) contain the following vulnerability:

fetchnews in leafnode 1.9.47 and earlier allows remote attackers to cause a denial of service (process hang) via an empty NNTP news article with missing mandatory headers.

CVE-2004-2068 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF leafnode-fetchnews-nntp-dos\(14189\)](#)

Secunia - Advisories - leafnode Missing Header Denial of Service Vulnerability

[Patch](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 10590](#)

[Patch](#)
[leafnode.sourceforge.net](#)
[text/plain](#)

[CONFIRM leafnode.sourceforge.net/leafnode-SA-2004-01.txt](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 3441](#)

Inactive Link **Not Archived**

No Description Provided

[web.archive.org](#)
[text/html](#)

[VULNWATCH 20040109 leafnode -1.9.47 security announcement SA-2004-01](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Leafnode	Leafnode	1.9.25	All	All	All
Application	Leafnode	Leafnode	1.9.26	All	All	All
Application	Leafnode	Leafnode	1.9.27	All	All	All
Application	Leafnode	Leafnode	1.9.28	All	All	All
Application	Leafnode	Leafnode	1.9.29	All	All	All
Application	Leafnode	Leafnode	1.9.30	All	All	All
Application	Leafnode	Leafnode	1.9.31	All	All	All
Application	Leafnode	Leafnode	1.9.32	All	All	All
Application	Leafnode	Leafnode	1.9.33	All	All	All
Application	Leafnode	Leafnode	1.9.34	All	All	All
Application	Leafnode	Leafnode	1.9.35	All	All	All
Application	Leafnode	Leafnode	1.9.36	All	All	All
Application	Leafnode	Leafnode	1.9.37	All	All	All
Application	Leafnode	Leafnode	1.9.38	All	All	All
Application	Leafnode	Leafnode	1.9.39	All	All	All
Application	Leafnode	Leafnode	1.9.40	All	All	All
Application	Leafnode	Leafnode	1.9.41	All	All	All
Application	Leafnode	Leafnode	1.9.42	All	All	All
Application	Leafnode	Leafnode	1.9.43	All	All	All
Application	Leafnode	Leafnode	1.9.44	All	All	All
Application	Leafnode	Leafnode	1.9.45	All	All	All
Application	Leafnode	Leafnode	1.9.46	All	All	All
Application	Leafnode	Leafnode	1.9.47	All	All	All
Application	Leafnode	Leafnode	1.9.25	All	All	All
Application	Leafnode	Leafnode	1.9.26	All	All	All
Application	Leafnode	Leafnode	1.9.27	All	All	All
Application	Leafnode	Leafnode	1.9.28	All	All	All

Application	Leafnode	Leafnode	1.9.29	All	All	All
Application	Leafnode	Leafnode	1.9.30	All	All	All
Application	Leafnode	Leafnode	1.9.31	All	All	All
Application	Leafnode	Leafnode	1.9.32	All	All	All
Application	Leafnode	Leafnode	1.9.33	All	All	All
Application	Leafnode	Leafnode	1.9.34	All	All	All
Application	Leafnode	Leafnode	1.9.35	All	All	All
Application	Leafnode	Leafnode	1.9.36	All	All	All
Application	Leafnode	Leafnode	1.9.37	All	All	All
Application	Leafnode	Leafnode	1.9.38	All	All	All
Application	Leafnode	Leafnode	1.9.39	All	All	All
Application	Leafnode	Leafnode	1.9.40	All	All	All
Application	Leafnode	Leafnode	1.9.41	All	All	All
Application	Leafnode	Leafnode	1.9.42	All	All	All
Application	Leafnode	Leafnode	1.9.43	All	All	All
Application	Leafnode	Leafnode	1.9.44	All	All	All
Application	Leafnode	Leafnode	1.9.45	All	All	All
Application	Leafnode	Leafnode	1.9.46	All	All	All
Application	Leafnode	Leafnode	1.9.47	All	All	All
cpe:2.3:a:leafnode:leafnode:1.9.25:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.26:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.27:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.28:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.29:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.30:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.31:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.32:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.33:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.34:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.35:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.36:*:*:*:*:*:						
cpe:2.3:a:leafnode:leafnode:1.9.37:*:*:*:*:*:						

cpe:2.3:a:leafnode:leafnode:1.9.38:*****:
cpe:2.3:a:leafnode:leafnode:1.9.39:*****:
cpe:2.3:a:leafnode:leafnode:1.9.40:*****:
cpe:2.3:a:leafnode:leafnode:1.9.41:*****:
cpe:2.3:a:leafnode:leafnode:1.9.42:*****:
cpe:2.3:a:leafnode:leafnode:1.9.43:*****:
cpe:2.3:a:leafnode:leafnode:1.9.44:*****:
cpe:2.3:a:leafnode:leafnode:1.9.45:*****:
cpe:2.3:a:leafnode:leafnode:1.9.46:*****:
cpe:2.3:a:leafnode:leafnode:1.9.47:*****:
cpe:2.3:a:leafnode:leafnode:1.9.25:*****:
cpe:2.3:a:leafnode:leafnode:1.9.26:*****:
cpe:2.3:a:leafnode:leafnode:1.9.27:*****:
cpe:2.3:a:leafnode:leafnode:1.9.28:*****:
cpe:2.3:a:leafnode:leafnode:1.9.29:*****:
cpe:2.3:a:leafnode:leafnode:1.9.30:*****:
cpe:2.3:a:leafnode:leafnode:1.9.31:*****:
cpe:2.3:a:leafnode:leafnode:1.9.32:*****:
cpe:2.3:a:leafnode:leafnode:1.9.33:*****:
cpe:2.3:a:leafnode:leafnode:1.9.34:*****:
cpe:2.3:a:leafnode:leafnode:1.9.35:*****:
cpe:2.3:a:leafnode:leafnode:1.9.36:*****:
cpe:2.3:a:leafnode:leafnode:1.9.37:*****:
cpe:2.3:a:leafnode:leafnode:1.9.38:*****:
cpe:2.3:a:leafnode:leafnode:1.9.39:*****:
cpe:2.3:a:leafnode:leafnode:1.9.40:*****:
cpe:2.3:a:leafnode:leafnode:1.9.41:*****:
cpe:2.3:a:leafnode:leafnode:1.9.42:*****:

cpe:2.3:a:leafnode:leafnode:1.9.43:*****:	
cpe:2.3:a:leafnode:leafnode:1.9.44:*****:	
cpe:2.3:a:leafnode:leafnode:1.9.45:*****:	
cpe:2.3:a:leafnode:leafnode:1.9.46:*****:	
cpe:2.3:a:leafnode:leafnode:1.9.47:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→