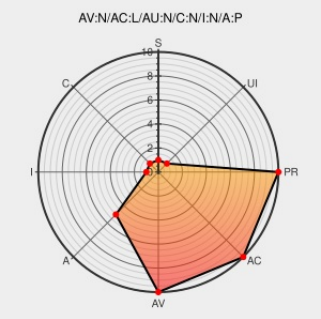
CVE-2002-1661

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1661

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Leafnode from Leafnode contain the following vulnerability:

The leafnode server in leafnode 1.9.20 to 1.9.29 allows remote attackers to cause a denial of service (infinite loop) when leafnode requests a cross-posted article to one group whose name is a prefix of another group.

CVE-2002-1661 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - Gentoo updates to leafnode	web.archive.org text/html	SECUNIA 7801
Secunia - Advisories - leafnode Denial of Service	web.archive.org text/html	SECUNIA 7799
Secunia - Advisories - Mandrake updates to leafnode	web.archive.org text/html	SECUNIA 7870
'Leafnode security announcement SA:2002:01' - MARC	marc.info text/html	BUGTRAQ 20021229 Leafnode security announcement SA:2002:01
	Patch leafnode.sourceforge.net text/plain	CONFIRM leafnode.sourceforge.net/leafnode-SA-2002-01.txt
Leafnode NNTP News Server Lets Remote Users Deny	www.securitytracker.com	SECTRACK 1005865

Service - SecurityTracker	text/html	
Leafnode Resource Exhaustion Denial Of Service Vulnerability	Patch cve.report (archive) text/html	BID 6490
'GLSA: leafnode' - MARC	marc.info text/html	BUGTRAQ 20030102 GLSA: leafnode
Mandriva Security Advisories	www.mandriva.com text/html	MANDRAKE MDKSA-2003:005
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF leafnode-nntp-dos(10942)

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	1.9.19	All	All	All
Application	Leafnode	Leafnode	1.9.20	All	All	All
Application	Leafnode	Leafnode	1.9.21	All	All	All
Application	Leafnode	Leafnode	1.9.22	All	All	All
Application	Leafnode	Leafnode	1.9.23	All	All	All
Application	Leafnode	Leafnode	1.9.24	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	1.9.29	All	All	All
Application	Leafnode	Leafnode	1.9.19	All	All	All
Application	Leafnode	Leafnode	1.9.20	All	All	All
Application	Leafnode	Leafnode	1.9.21	All	All	All
Application	Leafnode	Leafnode	1.9.22	All	All	All
Application	Leafnode	Leafnode	1.9.23	All	All	All
Application	Leafnode	Leafnode	1.9.24	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	1.9.29	All	All	All

cpe:2.3:a:leafnode:leafnode:1.9.19:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.20:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.21:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.22:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.23:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.24:*:*:*:*:*:*:*:

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:1.9.29:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.19:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.20:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.21:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.22:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.23:*:*:*:*:*:*:*:

cpe:2.3:a:leafnode:leafnode:1.9.24:*:*:*:*:*:*:*:

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:1.9.29:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→