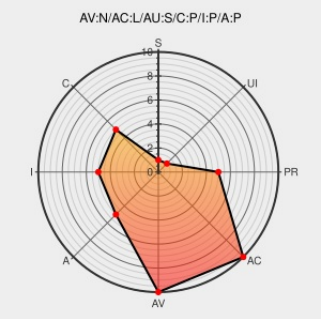
CVE-2009-4896

Published on: 08/02/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:38 AM UTC

CVE-2009-4896

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



Certain versions of Mlmmj from Mlmmj contain the following vulnerability:

Multiple directory traversal vulnerabilities in the mlmmj-php-admin web interface for Mailing List Managing Made Joyful (mlmmj) 1.2.15 through 1.2.17 allow remote authenticated users to overwrite, create, or delete arbitrary files, or determine the existence of arbitrary directories, via a .. (dot dot) in a list name in a (1) edit or (2) save action.

CVE-2009-4896 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian update for mlmmj - Advisories - Community	Vendor Advisory, web.archive.org, text/html	SECUNIA 40658
oss-security - CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	www.openwall.com, text/html	MLIST [oss-security] 20100623 CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
259968 – (CVE-2009-4896)	bugs.gentoo.org, text/html	CONFIRM bugs.gentoo.org/show_bug.cgi?id=259968
mlmmj ::	mlmmj.org, text/html, Inactive Link, Not Archived	CONFIRM mlmmj.org/node/84

oss-security - Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	Patch www.openwall.com text/html	MLIST [oss-security] 20100626 Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
oss-security - Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	www.openwall.com text/html	MLIST [oss-security] 20100704 Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
oss-security - Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	www.openwall.com text/html	MLIST [oss-security] 20100623 Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
oss-security - Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	www.openwall.com text/html	MLIST [oss-security] 20100706 Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
oss-security - Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface	www.openwall.com text/html	MLIST [oss-security] 20100625 Re: CVE Request -- mlmmj -- Directory traversal flaw by editing and saving list entries via php-admin web interface
Debian -- Security Information -- DSA-2073-1 mlmmj	www.debian.org Depreciated Link text/html	DEBIAN DSA-2073
Bug 607256 – CVE-2009-4896 mlmmj: Directory traversal flaw by editing and saving list entries via php-admin web interface	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=607256

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mlmmj	Mlmmj	1.2.15	All	All	All
Application	Mlmmj	Mlmmj	1.2.16	All	All	All
Application	Mlmmj	Mlmmj	1.2.17	All	All	All
Application	Mlmmj	Mlmmj	1.2.15	All	All	All
Application	Mlmmj	Mlmmj	1.2.16	All	All	All
Application	Mlmmj	Mlmmj	1.2.17	All	All	All

cpe:2.3:a:mlmmj:mlmmj:1.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:mlmmj:mlmmj:1.2.16:*:*:*:*:*:*:*:

cpe:2.3:a:mlmmj:mlmmj:1.2.17:*:*:*:*:*:*:*:

cpe:2.3:a:mlmmj:mlmmj:1.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:mlmmj:mlmmj:1.2.16:*:*:*:*:*:*:*

cpe:2.3:a:mlmmj:mlmmj:1.2.17:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→