



CVE-2002-0389

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2002-0389
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-06-18 04:00:00 UTC
Updated	2016-12-28 02:59:00 UTC
Description	Pipemail in Mailman stores private mail messages with predictable filenames in a world-executable directory, which allows

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Mailman	All	All	All	All
Application	Gnu	Mailman	All	All	All	All

References

Reference	Source	Link
Mailman / Bugs / #384 SECURITY: Pipemail permissions problem	MISC	s
Pipemail/Mailman Insecure Archives Permissions Vulnerability	BID	v
'Mailman/Pipemail private mailing list/local user vulnerability' - MARC	BUGTRAQ	r
Red Hat Customer Portal	REDHAT	r
ISS X-Force Database: pipemail-view-archives (8874): Pipemail could allow an attacker to view private mailing list archives	XF	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2016-12-27	Joshua Bressers	Red Hat does not intend to take any action on this issue. This is the expected behavior of M

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](#)