



CVE-2005-3573

Published on: 11/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

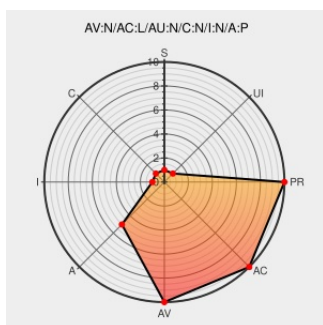
CVE-2005-3573

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Scrubber.py in Mailman 2.1.5-8 does not properly handle UTF8 character encodings in filenames of e-mail attachments, which allows remote attackers to cause a denial of service (application crash).

CVE-2005-3573 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

usn/usn-242-1 - Ubuntu Linux

www.ubuntu.com
[text/html](#)

[UBUNTU USN-242-1](#)

Secunia - Advisories - Mandriva update for mailman

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

[SECUNIA 17874](#)

Advisories - Mandriva

wwwnew.mandriva.com
[text/html](#)

[MANDRIVA MDKSA-2005:222](#)

Secunia - Advisories - Ubuntu update for mailman

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

[SECUNIA 18456](#)

Secunia - Advisories - Red Hat update for mailman

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

[SECUNIA 19167](#)

#327732 - Messages with invalid filenames don't get archived - Debian Bug report logs

bugs.debian.org
[text/html](#)

CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=327732

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10038
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2005-2404
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF mailman-utf8-scrubber-dos(23139)
Secunia - Advisories - Trustix update for mailman	web.archive.org text/html	 SECUNIA 19196
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0204
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20060401-01-U
[Mailman-Users] Uncaught runner exception: 'utf8' codeccan'tdecode bytes in position 1-4: invalid data	mail.python.org text/x-python	 MLIST [Mailman-Users] 20050912 Uncaught runner exception: 'utf8' codeccan'tdecode bytes in position 1-4: invalid data
GNU Mailman Attachment Scrubber UTF8 Filename Denial Of Service Vulnerability	cve.report (archive) text/html	 BID 15408
SecurityTracker.com Archives - GNU Mailman 'Scrubber.py' Decoding Error May Let Remote Users Deny Service	securitytracker.com text/html	 SECTrack 1015735
Secunia - Advisories - Debian update for mailman	web.archive.org text/html	 SECUNIA 18612
SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:001	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SR:2006:001
Secunia - Advisories - SUSE update for multiple packages	web.archive.org text/html	 SECUNIA 18503
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19532
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 20819
Secunia - Advisories - Mailman Attachment Filename Scrubbing Denial of Service	Vendor Advisory web.archive.org text/html	 SECUNIA 17511
Debian -- Security Information -- DSA-955-1 mailman	www.debian.org Deprecated Link text/html	 DEBIAN DSA-955
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX 2006-0012

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 OIDs associated with this CVE

There are currently no CVEs associated with this CPE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Mailman	2.0	beta3	All	All
Application	Gnu	Mailman	2.0	beta4	All	All
Application	Gnu	Mailman	2.0	beta5	All	All
Application	Gnu	Mailman	2.0.1	All	All	All
Application	Gnu	Mailman	2.0.10	All	All	All
Application	Gnu	Mailman	2.0.11	All	All	All
Application	Gnu	Mailman	2.0.12	All	All	All
Application	Gnu	Mailman	2.0.13	All	All	All
Application	Gnu	Mailman	2.0.14	All	All	All
Application	Gnu	Mailman	2.0.2	All	All	All
Application	Gnu	Mailman	2.0.3	All	All	All
Application	Gnu	Mailman	2.0.4	All	All	All
Application	Gnu	Mailman	2.0.5	All	All	All
Application	Gnu	Mailman	2.0.6	All	All	All
Application	Gnu	Mailman	2.0.7	All	All	All
Application	Gnu	Mailman	2.0.8	All	All	All
Application	Gnu	Mailman	2.0.9	All	All	All
Application	Gnu	Mailman	2.1	All	All	All
Application	Gnu	Mailman	2.1.1	beta1	All	All
Application	Gnu	Mailman	2.1.2	All	All	All
Application	Gnu	Mailman	2.1.3	All	All	All
Application	Gnu	Mailman	2.1.4	All	All	All
Application	Gnu	Mailman	2.1.5	All	All	All
Application	Gnu	Mailman	2.1.5.8	All	All	All
Application	Gnu	Mailman	2.0	beta3	All	All
Application	Gnu	Mailman	2.0	beta4	All	All
Application	Gnu	Mailman	2.0	beta5	All	All
Application	Gnu	Mailman	2.0.1	All	All	All
Application	Gnu	Mailman	2.0.10	All	All	All
Application	Gnu	Mailman	2.0.11	All	All	All
Application	Gnu	Mailman	2.0.12	All	All	All
Application	Gnu	Mailman	2.0.13	All	All	All

Application	Gnu	Mailman	2.0.14	All	All	All
Application	Gnu	Mailman	2.0.2	All	All	All
Application	Gnu	Mailman	2.0.3	All	All	All
Application	Gnu	Mailman	2.0.4	All	All	All
Application	Gnu	Mailman	2.0.5	All	All	All
Application	Gnu	Mailman	2.0.6	All	All	All
Application	Gnu	Mailman	2.0.7	All	All	All
Application	Gnu	Mailman	2.0.8	All	All	All
Application	Gnu	Mailman	2.0.9	All	All	All
Application	Gnu	Mailman	2.1	All	All	All
Application	Gnu	Mailman	2.1.1	beta1	All	All
Application	Gnu	Mailman	2.1.2	All	All	All
Application	Gnu	Mailman	2.1.3	All	All	All
Application	Gnu	Mailman	2.1.4	All	All	All
Application	Gnu	Mailman	2.1.5	All	All	All
Application	Gnu	Mailman	2.1.5.8	All	All	All
cpe:2.3:a:gnu:mailman:2.0:beta3:*****:						
cpe:2.3:a:gnu:mailman:2.0:beta4:*****:						
cpe:2.3:a:gnu:mailman:2.0:beta5:*****:						
cpe:2.3:a:gnu:mailman:2.0.1:*****:						
cpe:2.3:a:gnu:mailman:2.0.10:*****:						
cpe:2.3:a:gnu:mailman:2.0.11:*****:						
cpe:2.3:a:gnu:mailman:2.0.12:*****:						
cpe:2.3:a:gnu:mailman:2.0.13:*****:						
cpe:2.3:a:gnu:mailman:2.0.14:*****:						
cpe:2.3:a:gnu:mailman:2.0.2:*****:						
cpe:2.3:a:gnu:mailman:2.0.3:*****:						
cpe:2.3:a:gnu:mailman:2.0.4:*****:						
cpe:2.3:a:gnu:mailman:2.0.5:*****:						
cpe:2.3:a:gnu:mailman:2.0.6:*****:						
cpe:2.3:a:gnu:mailman:2.0.7:*****:						
cpe:2.3:a:gnu:mailman:2.0.8:*****:						

cpe:2.3:a:gnu:mailman:2.0.9:****:
cpe:2.3:a:gnu:mailman:2.1:****:
cpe:2.3:a:gnu:mailman:2.1.1:beta1:****:
cpe:2.3:a:gnu:mailman:2.1.2:****:
cpe:2.3:a:gnu:mailman:2.1.3:****:
cpe:2.3:a:gnu:mailman:2.1.4:****:
cpe:2.3:a:gnu:mailman:2.1.5:****:
cpe:2.3:a:gnu:mailman:2.1.5.8:****:
cpe:2.3:a:gnu:mailman:2.0:beta3:****:
cpe:2.3:a:gnu:mailman:2.0:beta4:****:
cpe:2.3:a:gnu:mailman:2.0:beta5:****:
cpe:2.3:a:gnu:mailman:2.0.1:****:
cpe:2.3:a:gnu:mailman:2.0.10:****:
cpe:2.3:a:gnu:mailman:2.0.11:****:
cpe:2.3:a:gnu:mailman:2.0.12:****:
cpe:2.3:a:gnu:mailman:2.0.13:****:
cpe:2.3:a:gnu:mailman:2.0.14:****:
cpe:2.3:a:gnu:mailman:2.0.2:****:
cpe:2.3:a:gnu:mailman:2.0.3:****:
cpe:2.3:a:gnu:mailman:2.0.4:****:
cpe:2.3:a:gnu:mailman:2.0.5:****:
cpe:2.3:a:gnu:mailman:2.0.6:****:
cpe:2.3:a:gnu:mailman:2.0.7:****:
cpe:2.3:a:gnu:mailman:2.0.8:****:
cpe:2.3:a:gnu:mailman:2.0.9:****:
cpe:2.3:a:gnu:mailman:2.1:****:
cpe:2.3:a:gnu:mailman:2.1.1:beta1:****:
cpe:2.3:a:gnu:mailman:2.1.2:****:

cpe:2.3:a:gnu:mailman:2.1.3:*****:
cpe:2.3:a:gnu:mailman:2.1.4:*****:
cpe:2.3:a:gnu:mailman:2.1.5:*****:
cpe:2.3:a:gnu:mailman:2.1.5.8:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)