

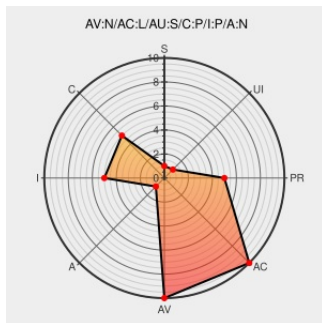


CVE-2010-3706

Published on: 10/06/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:18 AM UTC

CVE-2010-3706

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

plugins/acl/acl-backend-vfile.c in Dovecot 1.2.x before 1.2.15 and 2.0.x before 2.0.5 interprets an ACL entry as a directive to add to the permissions granted by another ACL entry, instead of a directive to replace the permissions granted by another ACL entry, in certain circumstances involving the private namespace of a user, which allows

remote authenticated users to bypass intended access restrictions via a request to read or modify a mailbox.

CVE-2010-3706 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

USN-1059-1: Dovecot vulnerabilities | Ubuntu

www.ubuntu.com
text/html

[UBUNTU USN-1059-1](#)

Support / Security / Advisories // MDVSA-2010:217 | Mandriva

www.mandriva.com
text/html

[MANDRIVA MDVSA-2010:217](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com
text/html

[VUPEN ADV-2010-2840](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com
text/html

[VUPEN ADV-2011-0301](#)

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:020	lists.opensuse.org text/html	 SUSE SUSE-SR:2010:020
'Re: [oss-security] CVE Request: more dovecot ACL issues' - MARC	marc.info text/html	 MLIST [oss-security] 20101004 Re: CVE Request: more dovecot ACL issues
[Dovecot] v1.2.15 released	Vendor Advisory www.dovecot.org text/html	 MLIST [dovecot] 20101002 v1.2.15 released
'[oss-security] CVE Request: more dovecot ACL issues' - MARC	marc.info text/html	 MLIST [oss-security] 20101004 CVE Request: more dovecot ACL issues
[Dovecot] ACL handling bugs in v1.2.8+ and v2.0	www.dovecot.org text/html	 MLIST [dovecot] 20101002 ACL handling bugs in v1.2.8+ and v2.0
Ubuntu update for dovecot - Secunia.com	web.archive.org text/html	 SECUNIA 43220
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2010-2572
[Dovecot] v2.0.5 released	Vendor Advisory www.dovecot.org text/html	 MLIST [dovecot] 20101002 v2.0.5 released

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	Dovecot	Dovecot	1.2.0	All	All	All
Application	Dovecot	Dovecot	1.2.1	All	All	All
Application	Dovecot	Dovecot	1.2.10	All	All	All
Application	Dovecot	Dovecot	1.2.11	All	All	All
Application	Dovecot	Dovecot	1.2.12	All	All	All
Application	Dovecot	Dovecot	1.2.13	All	All	All
Application	Dovecot	Dovecot	1.2.14	All	All	All
Application	Dovecot	Dovecot	1.2.2	All	All	All
Application	Dovecot	Dovecot	1.2.3	All	All	All
Application	Dovecot	Dovecot	1.2.4	All	All	All
Application	Dovecot	Dovecot	1.2.5	All	All	All
Application	Dovecot	Dovecot	1.2.6	All	All	All
Application	Dovecot	Dovecot	1.2.7	All	All	All
Application	Dovecot	Dovecot	1.2.8	All	All	All

Application	Dovecot	Dovecot	1.2.9	All	All	All
Application	Dovecot	Dovecot	2.0.0	All	All	All
Application	Dovecot	Dovecot	2.0.1	All	All	All
Application	Dovecot	Dovecot	2.0.2	All	All	All
Application	Dovecot	Dovecot	2.0.3	All	All	All
Application	Dovecot	Dovecot	2.0.4	All	All	All
Application	Dovecot	Dovecot	1.2.0	All	All	All
Application	Dovecot	Dovecot	1.2.1	All	All	All
Application	Dovecot	Dovecot	1.2.10	All	All	All
Application	Dovecot	Dovecot	1.2.11	All	All	All
Application	Dovecot	Dovecot	1.2.12	All	All	All
Application	Dovecot	Dovecot	1.2.13	All	All	All
Application	Dovecot	Dovecot	1.2.14	All	All	All
Application	Dovecot	Dovecot	1.2.2	All	All	All
Application	Dovecot	Dovecot	1.2.3	All	All	All
Application	Dovecot	Dovecot	1.2.4	All	All	All
Application	Dovecot	Dovecot	1.2.5	All	All	All
Application	Dovecot	Dovecot	1.2.6	All	All	All
Application	Dovecot	Dovecot	1.2.7	All	All	All
Application	Dovecot	Dovecot	1.2.8	All	All	All
Application	Dovecot	Dovecot	1.2.9	All	All	All
Application	Dovecot	Dovecot	2.0.0	All	All	All
Application	Dovecot	Dovecot	2.0.1	All	All	All
Application	Dovecot	Dovecot	2.0.2	All	All	All
Application	Dovecot	Dovecot	2.0.3	All	All	All
Application	Dovecot	Dovecot	2.0.4	All	All	All
cpe:2.3:a:dovecot:dovecot:1.2.0:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.1:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.10:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.11:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.12:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.13:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.14:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.2:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.3:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.4:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.5:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.6:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.7:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.8:****:*:*:						
cpe:2.3:a:dovecot:dovecot:1.2.9:****:*:*:						
cpe:2.3:a:dovecot:dovecot:2.0.0:****:*:*:						
cpe:2.3:a:dovecot:dovecot:2.0.1:****:*:*:						
cpe:2.3:a:dovecot:dovecot:2.0.2:****:*:*:						
cpe:2.3:a:dovecot:dovecot:2.0.3:****:*:*:						
cpe:2.3:a:dovecot:dovecot:2.0.4:****:*:*:						

cpe:2.3:a:dovecot:dovecot:1.2.2:*****:
cpe:2.3:a:dovecot:dovecot:1.2.3:*****:
cpe:2.3:a:dovecot:dovecot:1.2.4:*****:
cpe:2.3:a:dovecot:dovecot:1.2.5:*****:
cpe:2.3:a:dovecot:dovecot:1.2.6:*****:
cpe:2.3:a:dovecot:dovecot:1.2.7:*****:
cpe:2.3:a:dovecot:dovecot:1.2.8:*****:
cpe:2.3:a:dovecot:dovecot:1.2.9:*****:
cpe:2.3:a:dovecot:dovecot:2.0.0:*****:
cpe:2.3:a:dovecot:dovecot:2.0.1:*****:
cpe:2.3:a:dovecot:dovecot:2.0.2:*****:
cpe:2.3:a:dovecot:dovecot:2.0.3:*****:
cpe:2.3:a:dovecot:dovecot:2.0.4:*****:
cpe:2.3:a:dovecot:dovecot:1.2.0:*****:
cpe:2.3:a:dovecot:dovecot:1.2.1:*****:
cpe:2.3:a:dovecot:dovecot:1.2.10:*****:
cpe:2.3:a:dovecot:dovecot:1.2.11:*****:
cpe:2.3:a:dovecot:dovecot:1.2.12:*****:
cpe:2.3:a:dovecot:dovecot:1.2.13:*****:
cpe:2.3:a:dovecot:dovecot:1.2.14:*****:
cpe:2.3:a:dovecot:dovecot:1.2.2:*****:
cpe:2.3:a:dovecot:dovecot:1.2.3:*****:
cpe:2.3:a:dovecot:dovecot:1.2.4:*****:
cpe:2.3:a:dovecot:dovecot:1.2.5:*****:
cpe:2.3:a:dovecot:dovecot:1.2.6:*****:
cpe:2.3:a:dovecot:dovecot:1.2.7:*****:
cpe:2.3:a:dovecot:dovecot:1.2.8:*****:
cpe:2.3:a:dovecot:dovecot:1.2.9:*****:
cpe:2.3:a:dovecot:dovecot:2.0.0:*****:

cpe:2.3:a:dovecot:dovecot:2.0.1:*****:
cpe:2.3:a:dovecot:dovecot:2.0.2:*****:
cpe:2.3:a:dovecot:dovecot:2.0.3:*****:
cpe:2.3:a:dovecot:dovecot:2.0.4:*****:

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](#)