



CVE-2008-1199

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

Summary

CVE	CVE-2008-1199
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-06 21:44:00 UTC
Updated	2018-10-11 20:30:00 UTC
Description	Dovecot before 1.0.11, when configured to use mail_extra_groups to allow Dovecot to create dotlocks in /var/mail, might all

Risk And Classification

Problem Types: CWE-16 | CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dovecot	Dovecot	0.99.13	All	All	All
Application	Dovecot	Dovecot	0.99.14	All	All	All
Application	Dovecot	Dovecot	1.0	All	All	All
Application	Dovecot	Dovecot	1.0.10	All	All	All
Application	Dovecot	Dovecot	1.0.2	All	All	All
Application	Dovecot	Dovecot	1.0.3	All	All	All
Application	Dovecot	Dovecot	1.0.4	All	All	All
Application	Dovecot	Dovecot	1.0.5	All	All	All
Application	Dovecot	Dovecot	1.0.6	All	All	All
Application	Dovecot	Dovecot	1.0.7	All	All	All
Application	Dovecot	Dovecot	1.0.8	All	All	All
Application	Dovecot	Dovecot	1.0.9	All	All	All
Application	Dovecot	Dovecot	1.0.beta2	All	All	All
Application	Dovecot	Dovecot	1.0.beta3	All	All	All
Application	Dovecot	Dovecot	1.0.beta7	All	All	All
Application	Dovecot	Dovecot	1.0.beta8	All	All	All
Application	Dovecot	Dovecot	1.0.rc1	All	All	All

Application	Dovecot	Dovecot	1.0.rc10	All	All	All
Application	Dovecot	Dovecot	1.0.rc11	All	All	All
Application	Dovecot	Dovecot	1.0.rc12	All	All	All
Application	Dovecot	Dovecot	1.0.rc13	All	All	All
Application	Dovecot	Dovecot	1.0.rc14	All	All	All
Application	Dovecot	Dovecot	1.0.rc15	All	All	All
Application	Dovecot	Dovecot	1.0.rc2	All	All	All
Application	Dovecot	Dovecot	1.0.rc3	All	All	All
Application	Dovecot	Dovecot	1.0.rc4	All	All	All
Application	Dovecot	Dovecot	1.0.rc5	All	All	All
Application	Dovecot	Dovecot	1.0.rc6	All	All	All
Application	Dovecot	Dovecot	1.0.rc7	All	All	All
Application	Dovecot	Dovecot	1.0.rc8	All	All	All
Application	Dovecot	Dovecot	1.0.rc9	All	All	All
Application	Dovecot	Dovecot	1.0_rc29	All	All	All
Application	Dovecot	Dovecot	0.99.13	All	All	All
Application	Dovecot	Dovecot	0.99.14	All	All	All
Application	Dovecot	Dovecot	1.0	All	All	All
Application	Dovecot	Dovecot	1.0.10	All	All	All
Application	Dovecot	Dovecot	1.0.2	All	All	All
Application	Dovecot	Dovecot	1.0.3	All	All	All
Application	Dovecot	Dovecot	1.0.4	All	All	All
Application	Dovecot	Dovecot	1.0.5	All	All	All
Application	Dovecot	Dovecot	1.0.6	All	All	All
Application	Dovecot	Dovecot	1.0.7	All	All	All
Application	Dovecot	Dovecot	1.0.8	All	All	All
Application	Dovecot	Dovecot	1.0.9	All	All	All
Application	Dovecot	Dovecot	1.0.beta2	All	All	All
Application	Dovecot	Dovecot	1.0.beta3	All	All	All
Application	Dovecot	Dovecot	1.0.beta7	All	All	All
Application	Dovecot	Dovecot	1.0.beta8	All	All	All
Application	Dovecot	Dovecot	1.0.rc1	All	All	All
Application	Dovecot	Dovecot	1.0.rc10	All	All	All
Application	Dovecot	Dovecot	1.0.rc11	All	All	All
Application	Dovecot	Dovecot	1.0.rc12	All	All	All

Application	Dovecot	Dovecot	1.0.rc13	All	All	All
Application	Dovecot	Dovecot	1.0.rc14	All	All	All
Application	Dovecot	Dovecot	1.0.rc15	All	All	All
Application	Dovecot	Dovecot	1.0.rc2	All	All	All
Application	Dovecot	Dovecot	1.0.rc3	All	All	All
Application	Dovecot	Dovecot	1.0.rc4	All	All	All
Application	Dovecot	Dovecot	1.0.rc5	All	All	All
Application	Dovecot	Dovecot	1.0.rc6	All	All	All
Application	Dovecot	Dovecot	1.0.rc7	All	All	All
Application	Dovecot	Dovecot	1.0.rc8	All	All	All
Application	Dovecot	Dovecot	1.0.rc9	All	All	All
Application	Dovecot	Dovecot	1.0_rc29	All	All	All

References						
Reference				Source	Link	
Dovecot: Multiple vulnerabilities — Gentoo Linux Documentation				GENTOO	security.gentoo.o	
Repository / Oval Repository				OVAL	oval.cisecurity.org	
[SECURITY] Fedora 7 Update: dovecot-1.0.13-18.fc7				FEDORA	www.redhat.com	
Dovecot 'mail_extra_groups' Insecure Settings Local Unauthorized Access Vulnerability				BID	www.securityfocu	
Red Hat update for dovecot - Advisories - Secunia				SECUNIA	secunia.com	
SUSE update for dovecot and graphicsmagic - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia.com	
[SECURITY] Fedora 8 Update: dovecot-1.0.13-6.fc8				FEDORA	www.redhat.com	
Debian update for dovecot - Advisories - Secunia				SECUNIA	secunia.com	
[Dovecot-news] v1.0.11 released				MLIST	www.dovecot.org	
Ubuntu update for dovecot - Advisories - Secunia				SECUNIA	secunia.com	
Fedora update for dovecot - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia.com	
IBM X-Force Exchange				XF	exchange.xforce.	
USN-593-1: Dovecot vulnerabilities Ubuntu security notices				UBUNTU	usn.ubuntu.com	
Gentoo update for dovecot - Advisories - Secunia				SECUNIA	secunia.com	
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:020				SUSE	lists.opensuse.or	
SecurityFocus				BUGTRAQ	www.securityfocu	
Support				REDHAT	www.redhat.com	
Debian -- Security Information -- DSA-1516-1 dovecot				DEBIAN	www.debian.org	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-05-21	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/show_bug.cgi?id=444189

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