



# CVE-2017-15132

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

## Summary

<b>CVE</b>	CVE-2017-15132
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-01-25 20:29:00 UTC
<b>Updated</b>	2019-10-09 23:24:00 UTC
<b>Description</b>	A flaw was found in dovecot 2.0 up to 2.2.33 and 2.3.0. An abort of SASL authentication results in a memory leak in dovecc

## Risk And Classification

### Problem Types: CWE-772

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Dovecot</a>	<a href="#">Dovecot</a>	2.3.0	All	All	All
Application	<a href="#">Dovecot</a>	<a href="#">Dovecot</a>	2.3.0	All	All	All
Application	<a href="#">Dovecot</a>	<a href="#">Dovecot</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4130-1 dovecot	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party
USN-3556-1: Dovecot vulnerability   Ubuntu security notices	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party
USN-3556-2: Dovecot vulnerabilities   Ubuntu security notices	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party
[Dovecot-news] v2.2.34 released	MLIST	<a href="http://www.dovecot.org">www.dovecot.org</a>	Vendor
Bug 1532768 – CVE-2017-15132 dovecot: Auth leaks memory if SASL authentication is aborted	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracker
[SECURITY] [DLA 1333-1] dovecot security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List
<a href="https://github.com/dovecot/core/commit/1a29ed2f96da1be22fa5a4d96c7583aa81b8b060...">github.com/dovecot/core/commit/1a29ed2f96da1be22fa5a4d96c7583aa81b8b060...</a>	CONFIRM	<a href="http://github.com">github.com</a>	Patch, Commit
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500152](#) Alpine Linux Security Update for dovecot

[503802](#) Alpine Linux Security Update for dovecot

© [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](#).

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