



# CVE-2020-15011

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

## Summary

<b>CVE</b>	CVE-2020-15011
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-24 12:15:00 UTC
<b>Updated</b>	2021-11-30 22:29:00 UTC
<b>Description</b>	GNU Mailman before 2.1.33 allows arbitrary content injection via the Cgi/private.py private archive login page.

## Risk And Classification

**Problem Types:** CWE-74

## 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>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	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>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	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>	8.0	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Mailman</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Mailman</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1752-1: moderate: Recommended updat	SUSE	<a href="#">lists.opensuse.org</a>	
Debian -- Security Information -- DSA-4991-1 mailman	DEBIAN	<a href="#">www.debian.org</a>	
[SECURITY] [DLA 2276-1] mailman security update	MLIST	<a href="#">lists.debian.org</a>	
USN-4406-1: Mailman vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>	Third Party Ac
[SECURITY] [DLA 2285-1] mailman security update	MLIST	<a href="#">lists.debian.org</a>	Mailing List T

[SECURITY] [DLA 2203-1] mailman security update	MISC	<a href="https://lists.debian.org">lists.debian.org</a>	mailing list, p...
Bug #1877379 "Arbitrary Content Injection via the private archiv..." : Bugs : GNU Mailman	MISC	<a href="https://bugs.launchpad.net">bugs.launchpad.net</a>	Issue Tracking
[security-announce] openSUSE-SU-2020:1707-1: moderate: Recommended updat	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159210](#) Oracle Enterprise Linux Security Update for mailman:2.1 (ELSA-2021-1751)

[178829](#) Debian Security Update for mailman (DSA 4991-1)

[198576](#) Ubuntu Security Notification for Mailman Vulnerabilities (USN-5121-2)

[239311](#) Red Hat Update for mailman:2.1 (RHSA-2021:1751)

[377570](#) Alibaba Cloud Linux Security Update for mailman:2.1 (ALINUX3-SA-2022:0093)

[940352](#) AlmaLinux Security Update for mailman:2.1 (ALSA-2021:1751)

[960755](#) Rocky Linux Security Update for mailman:2.1 (RLSA-2021:1751)

© [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](#)