



# CVE-2019-3878

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-3878
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-26 18:29:00 UTC
<b>Updated</b>	2023-11-07 03:10:00 UTC
<b>Description</b>	A vulnerability was found in mod_auth_mellon before v0.14.2. If Apache is configured as a reverse proxy and mod_auth_m

## Risk And Classification

**Problem Types:** CWE-287

## 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>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	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>	18.10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Application	<a href="#">Mod Auth Mellon Project</a>	<a href="#">Mod Auth Mellon</a>	All	All	All	All
Application	<a href="#">Mod Auth Mellon Project</a>	<a href="#">Mod Auth Mellon</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 30 Update: mod_auth_mellon-0.14.2-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: mod_auth_mellon-0.14.2-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
Modify am_handler setup to run before mod_proxy by jhrozek · Pull Request #196 · Uninett/mod_auth_mellon · GitHub	CONFIRM	<a href="#">github.com</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
[SECURITY] Fedora 29 Update: mod_auth_mellon-0.14.0-5.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 29 Update: mod_auth_mellon-0.14.0-5.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
1691126 – (CVE-2019-3878) CVE-2019-3878 mod_auth_mellon: authentication bypass in ECP flow	CONFIRM	<a href="#">bugzilla.redhat.com</a>
USN-3924-1: mod_auth_mellon vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377002](#) Alibaba Cloud Linux Security Update for mod\_auth\_mellon (ALINUX2-SA-2019:0021)

[377582](#) Alibaba Cloud Linux Security Update for mod\_auth\_mellon (ALINUX3-SA-2022:0100)

[378300](#) Virtuozzo Linux Security Update for mod\_auth\_mellon-diagnostics (VZLSA-2019:0766)

© 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](#)**