



# CVE-2021-3639

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

## Summary

<b>CVE</b>	CVE-2021-3639
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-22 15:15:00 UTC
<b>Updated</b>	2023-02-12 23:41:00 UTC
<b>Description</b>	A flaw was found in mod_auth_mellon where it does not sanitize logout URLs properly. This issue could be used by an atta

## Risk And Classification

**Problem Types:** CWE-601

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uninett	Mod Auth Mellon	All	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.co</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.co</a>
Prevent redirect to URLs that begin with '///' · latchset/mod_auth_mellon@42a1126 · GitHub	MISC	<a href="#">github.com</a>
1980648 – (CVE-2021-3639) CVE-2021-3639 mod_auth_mellon: Open Redirect vulnerability in logout URLs	MISC	<a href="#">bugzilla.redhat.co</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

159805 Oracle Enterprise Linux Security Update for mod\_auth\_mellon (ELSA-2022-1934)

181385 Debian Security Update for libapache2-mod-auth-mellon (CVE-2021-3639)

101000 Debian Security Update for libapache2-mod-auth-mellon (CVE-2021-3639)

<a href="#">181628</a> Debian Security Update for libapache2-mod-auth-mellon (DLA 3359-1)
<a href="#">198485</a> Ubuntu Security Notification for mod-auth-mellon Vulnerability (USN-5069-2)
<a href="#">198496</a> Ubuntu Security Notification for mod-auth-mellon Vulnerability (USN-5069-1)
<a href="#">240312</a> Red Hat Update for mod_auth_mellon (RHSA-2022:1934)
<a href="#">282204</a> Fedora Security Update for mod_auth_mellon (FEDORA-2021-5e033d6641)
<a href="#">282229</a> Fedora Security Update for mod_auth_mellon (FEDORA-2022-b18f01985a)
<a href="#">355386</a> Amazon Linux Security Advisory for mod_auth_mellon : ALAS2-2023-2077
<a href="#">355426</a> Amazon Linux Security Advisory for mod24_auth_mellon : ALAS-2023-1765
<a href="#">670753</a> EulerOS Security Update for mod_auth_mellon (EulerOS-SA-2021-2511)
<a href="#">671018</a> EulerOS Security Update for mod_auth_mellon (EulerOS-SA-2021-2597)
<a href="#">671432</a> EulerOS Security Update for mod_auth_mellon (EulerOS-SA-2022-1354)
<a href="#">751076</a> SUSE Enterprise Linux Security Update for apache2-mod_auth_mellon (SUSE-SU-2021:2912-1)
<a href="#">752106</a> SUSE Enterprise Linux Security Update for apache2-mod_auth_mellon (SUSE-SU-2022:1524-1)
<a href="#">903886</a> Common Base Linux Mariner (CBL-Mariner) Security Update for mod_auth_mellon (10651)
<a href="#">907262</a> Common Base Linux Mariner (CBL-Mariner) Security Update for mod_auth_mellon (10651-1)
<a href="#">940560</a> AlmaLinux Security Update for mod_auth_mellon (ALSA-2022:1934)
<a href="#">960334</a> Rocky Linux Security Update for mod_auth_mellon (RLSA-2022:1934)

© [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](#)**