



# CVE-2021-32785

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

## Summary

<b>CVE</b>	CVE-2021-32785
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-22 22:15:00 UTC
<b>Updated</b>	2024-01-30 20:47:00 UTC
<b>Description</b>	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID

## Risk And Classification

**Problem Types:** CWE-134

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Openidc</a>	<a href="#">Mod Auth Openidc</a>	All	All	All	All
Application	<a href="#">Zmartzone</a>	<a href="#">Mod Auth Openidc</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 3409-1] libapache2-mod-auth-openidc security update	MLIST	<a href="#">lists.debian.org</a>
Merge pull request from GHSA-55r8-6w97-xxr4 · zmartzone/mod_auth_openidc@dc67268 · GitHub	MISC	<a href="#">github.com</a>
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="#">www.oracle.com</a>
Format string bug in the Redis cache implementation · Advisory · zmartzone/mod_auth_openidc · GitHub	CONFIRM	<a href="#">github.com</a>
Release release 2.4.9 · zmartzone/mod_auth_openidc · GitHub	MISC	<a href="#">github.com</a>
July 2021 Apache HTTP Server Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.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

[179645](#) Debian Security Update for libapache2-mod-auth-openidc (CVE-2021-32785)

[181758](#) Debian Security Update for libapache2-mod-auth-openidc (DLA 3409-1)

[751134](#) OpenSUSE Security Update for apache2-mod\_auth\_openidc (openSUSE-SU-2021:3020-1)

[751149](#) OpenSUSE Security Update for apache2-mod\_auth\_openidc (openSUSE-SU-2021:1277-1)

[751211](#) SUSE Enterprise Linux Security Update for apache2-mod\_auth\_openidc (SUSE-SU-2021:3352-1)

[901284](#) Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6479-1)

© [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](#)