



# CVE-2021-32786

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

## Summary

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-32786                                                                                                        |
| <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>         | 2023-11-07 03:35:00 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-601

## 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="#">Fedoraproject</a> | <a href="#">Fedora</a>           | 33      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>           | 34      | 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>        |
| [SECURITY] Fedora 33 Update: mod_auth_openidc-2.4.9-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="#">lists.fedoraproject.org</a> |
| Oracle Critical Patch Update Advisory - April 2022                                                   | MISC    | <a href="#">www.oracle.com</a>          |
| Release release 2.4.9 · zmartzone/mod_auth_openidc · GitHub                                          | MISC    | <a href="#">github.com</a>              |
| [SECURITY] Fedora 33 Update: mod_auth_openidc-2.4.9-1.fc33 - package-announce - Fedora Mailing-Lists |         | <a href="#">lists.fedoraproject.org</a> |
| July 2021 Apache HTTP Server Vulnerabilities in NetApp Products   NetApp Product Security            | CONFIRM | <a href="#">security.netapp.com</a>     |
| [SECURITY] Fedora 34 Update: mod_auth_openidc-2.4.9-1.fc34 - package-announce - Fedora Mailing-Lists |         | <a href="#">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 34 Update: mod_auth_openidc-2.4.9-1.fc34 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="#">lists.fedoraproject.org</a> |
| Merge pull request from GHSA-xm4c-5wm5-jqv7 · zmartzone/mod_auth_openidc@3a11548 · GitHub            | MISC    | <a href="#">github.com</a>              |

|                                                                                                |         |                                                     |
|------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------|
| One URL standard please   daniel.haxx.se                                                       | MISC    | <a href="https://daniel.haxx.se">daniel.haxx.se</a> |
| Open Redirect in oidc_validate_redirect_url() · Advisory · zmartzone/mod_auth_openidc · GitHub | CONFIRM | <a href="https://github.com">github.com</a>         |
| CVE Program record                                                                             | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>       |
| NVD vulnerability detail                                                                       | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

|                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">159800</a> Oracle Enterprise Linux Security Update for mod_auth_openidc:2.3 (ELSA-2022-1823)        |
| <a href="#">179805</a> Debian Security Update for libapache2-mod-auth-openidc (CVE-2021-32786)                  |
| <a href="#">181758</a> Debian Security Update for libapache2-mod-auth-openidc (DLA 3409-1)                      |
| <a href="#">240273</a> Red Hat Update for mod_auth_openidc:2.3 (RHSA-2022:1823)                                 |
| <a href="#">281777</a> Fedora Security Update for mod_auth_openidc (FEDORA-2021-17f5cedf66)                     |
| <a href="#">281778</a> Fedora Security Update for mod_auth_openidc (FEDORA-2021-e3017c538a)                     |
| <a href="#">377581</a> Alibaba Cloud Linux Security Update for mod_auth_openidc:2.3 (ALINUX3-SA-2022:0135)      |
| <a href="#">751134</a> OpenSUSE Security Update for apache2-mod_auth_openidc (openSUSE-SU-2021:3020-1)          |
| <a href="#">751149</a> OpenSUSE Security Update for apache2-mod_auth_openidc (openSUSE-SU-2021:1277-1)          |
| <a href="#">751211</a> SUSE Enterprise Linux Security Update for apache2-mod_auth_openidc (SUSE-SU-2021:3352-1) |
| <a href="#">901439</a> Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6480-1)               |
| <a href="#">940537</a> AlmaLinux Security Update for mod_auth_openidc:2.3 (ALSA-2022:1823)                      |
| <a href="#">960287</a> Rocky Linux Security Update for mod_auth_openidc:2.3 (RLSA-2022:1823)                    |

© [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](https://status.cve.report)