



CVE-2023-28625

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

Summary

CVE	CVE-2023-28625
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-03 14:15:00 UTC
Updated	2023-05-31 20:15:00 UTC
Description	mod_auth_openidc is an authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect protocol.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Openidc	Mod Auth Openidc	All	All	All	All

References

Reference	Score
segfault DoS when OI DCStripCookies is set · Advisory · OpenIDC/mod_auth_openidc · GitHub	MI
Debian -- Security Information -- DSA-5405-1 libapache2-mod-auth-openidc	MI
2.4.13.2: prevent DoS core dump with OI DCStripCookies; CVE-2023-28625 · OpenIDC/mod_auth_openidc@c0e1eda · GitHub	MI
[SECURITY] Fedora 38 Update: mod_auth_openidc-2.4.13.2-1.fc38 - package-announce - Fedora Mailing-Lists	MI
Release release 2.4.13.2 · OpenIDC/mod_auth_openidc · GitHub	MI
[SECURITY] [DLA 3409-1] libapache2-mod-auth-openidc security update	MI
mod_auth_openidc/src/mod_auth_openidc.c at 3f11976dab56af0a46a7dddb7a275cc16d6eb726 · OpenIDC/mod_auth_openidc · GitHub	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161083 Oracle Enterprise Linux Security Update for mod_auth_openidc (ELSA-2023-6365)
161183 Oracle Enterprise Linux Security Update for mod_auth_openidc:2.3 (ELSA-2023-6940)
181758 Debian Security Update for libapache2-mod-auth-openidc (DLA 3409-1)
181791 Debian Security Update for libapache2-mod-auth-openidc (DSA 5405-1)
181985 Debian Security Update for libapache2-mod-auth-openidc (CVE-2023-28625)
242302 Red Hat Update for mod_auth_openidc (RHSA-2023:6365)
242410 Red Hat Update for mod_auth_openidc:2.3 (RHSA-2023:6940)
284103 Fedora Security Update for mod_auth_openidc (FEDORA-2023-b534ca7056)
753913 SUSE Enterprise Linux Security Update for apache2-mod_auth_openidc (SUSE-SU-2023:1849-1)
753996 SUSE Enterprise Linux Security Update for apache2-mod_auth_openidc (SUSE-SU-2023:1837-1)
907302 Common Base Linux Mariner (CBL-Mariner) Security Update for mod_auth_openidc (26772-1)
941392 AlmaLinux Security Update for mod_auth_openidc (ALSA-2023:6365)
941476 AlmaLinux Security Update for mod_auth_openidc:2.3 (ALSA-2023:6940)

© [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](#)