



CVE-2021-20718

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-20718
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-20 02:15:00 UTC
Updated	2023-11-07 03:29:00 UTC
Description	mod_auth_openidc 2.4.0 to 2.4.7 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vect

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Openidc	Mod Auth Openidc	All	All	All	All
Application	Oracle	Essbase	All	All	All	All
Application	Zmartzone	Mod Auth Openidc	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: mod_auth_openidc-2.4.8.4-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedo
JVN#49704918: mod_auth_openidc vulnerable to denial-of-service (DoS)	MISC	jvn.jp
GitHub - zmartzone/mod_auth_openidc: OpenID Connect Relying Party implementation for Apache HTTP Server 2.x	MISC	github.co
Oracle Critical Patch Update Advisory - January 2022	MISC	www.ora
[SECURITY] Fedora 34 Update: mod_auth_openidc-2.4.8.4-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedo
[SECURITY] Fedora 33 Update: mod_auth_openidc-2.4.8.4-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedo
[SECURITY] Fedora 34 Update: mod_auth_openidc-2.4.8.4-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedo
Z m a r t Z o n e	MISC	www.zma
CVE Program record	CVE.ORG	www.cve

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179767](#) Debian Security Update for libapache2-mod-auth-openidc (CVE-2021-20718)

[281623](#) Fedora Security Update for mod_auth_openidc (FEDORA-2021-cc85f79f63)

[281624](#) Fedora Security Update for mod_auth_openidc (FEDORA-2021-46b017b771)

[376367](#) Oracle Essbase Administration Services Security Update (CPUJAN2022)

[750132](#) SUSE Enterprise Linux Security Update for apache2-mod_auth_openidc (SUSE-SU-2021:1900-1)

[901210](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mod_auth_openidc (7288)

[907269](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mod_auth_openidc (7288-1)

© [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](#)