



CVE-2021-32791

Published on: 07/26/2021 12:00:00 AM UTC

Last Modified on: 08/09/2021 05:59:00 PM UTC

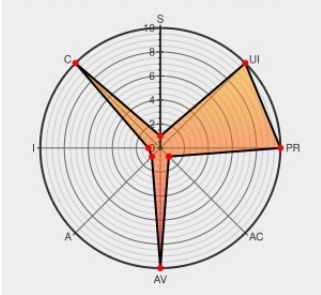
CVE-2021-32791 - advisory for GHSA-px3c-6x7j-3r9r

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix

because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjson AES encryption routines.

CVE-2021-32791 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [zmartzone](#) - `mod_auth_openidc` version < 2.4.9






CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
use encrypted JWTs for storing encrypted cache contents · zmartzone/mod_auth_openidc@375407c · GitHub	github.com text/html	 MISC github.com/zmartzone/mod_auth_openidc/commit/375407c16c61a70b56fc
[SECURITY] Fedora 33 Update: mod_auth_openidc-2.4.9-1.fc33 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-17f5cedf66
Hardcoded static IV and AAD with a reused key in AES GCM encryption · Advisory · zmartzone/mod_auth_openidc · GitHub	github.com text/html	 CONFIRM github.com/zmartzone/mod_auth_openidc/security/advisorie
Release release 2.4.9 · zmartzone/mod_auth_openidc · GitHub	github.com text/html	 MISC github.com/zmartzone/mod_auth_openidc/releases/tag/v2.4.9
[SECURITY] Fedora 34 Update: mod_auth_openidc-2.4.9-1.fc34 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-e3017c538a

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [281777](#) Fedora Security Update for mod_auth_openidc (FEDORA-2021-17f5cedf66)
- [281778](#) Fedora Security Update for mod_auth_openidc (FEDORA-2021-e3017c538a)
- [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)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Zmartzone	Mod Auth Openidc	All	All	All	All

```
cpe:2.3:a:apache:http_server:*.:*:*:*:*:
```


```
cpe:2.3:o:fedoraproject:fedora:33:*.:*:*:*:
```

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:

cpe:2.3:a:zmartzone:mod_auth_openidc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2021-32791 : mod_auth_openidc is an authentication/authorization module for the #Apache 2.x HTTP server that fu... twitter.com/i/web/status/1...	2021-07-26 17:08:28

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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