

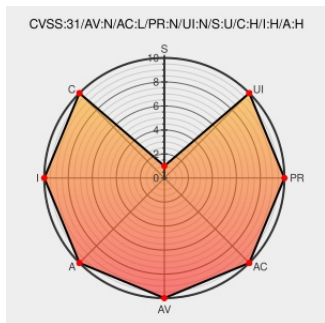


CVE-2020-36599

Published on: Not Yet Published

Last Modified on: 08/19/2022 04:25:00 PM UTC

CVE-2020-36599

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Omniauth](#) from [Omniauth](#) contain the following vulnerability:

lib/omniauth/failure_endpoint.rb in OmniAuth before 1.9.2 (and before 2.0) does not escape the message_key value.

CVE-2020-36599 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality
Impact

Integrity
Impact

Availability
Impact

UNCHANGED

HIGH

HIGH

HIGH

CVE References

Description

Tags

Link

Merge branch '2_0-indev' into
fix-path-prefix-when-
redirecting-on-fai...
omniauth/omniauth@43a396f
· GitHub

[github.com](#)
[text/html](#)

MISC

github.com/omniauth/omniauth/commit/43a396f181ef7d0ed2ec8291c939c95e3ed3ff00#diff-575abda9deb9b1a77bf534e898a923029b9a61e991d626db88dc6e8b34260aa2

omniauth | RubyGems.org |
your community gem host

[rubygems.org](#)
[text/html](#)

MISC rubygems.org/gems/omniauth/versions/1.9.2

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

lib/omniauth/failure_endpoint.rb in OmniAuth before 1.9.2 (and before 2.0) does not escape the message_key value. CVE...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Omniauth	Omniauth	All	All	All	All
cpe:2.3:a:omniauth:omniauth:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-36599 : lib/omniauth/failure_endpoint.rb in OmniAuth before 2.0 does not escape the message_key value.... cve.report/CVE-2020-36599	2022-08-18 23:06:06
 /r/netcve	CVE-2020-36599	2022-08-19 00:38:21

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)