



CVE-2020-7787

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7787

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

SS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RL:T/R



Certain versions of [React-adal](#) from [React-adal Project](#) contain the following vulnerability:

This affects all versions of package react-adal. It is possible for a specially crafted JWT token and request URL can cause the nonce, session and refresh values to be incorrectly validated, causing the application to treat an attacker-generated JWT token as authentic. The logical defect is caused by how the nonce, session and refresh values

are stored in the browser local storage or session storage. Each key is automatically appended by ||. When the received nonce and session keys are generated, the list of values is stored in the browser storage, separated by ||, with || always appended to the end of the list. Since || will always be the last 2 characters of the stored values, an empty string ("") will always be in the list of the valid values. Therefore, if an empty session parameter is provided in the callback URL, and a specially-crafted JWT token contains an nonce value of "" (empty string), then adal.js will consider the JWT token as authentic.

CVE-2020-7787 has been assigned by report@snyk.io to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.2 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
ADAL.js update by krishardy · Pull Request #115 · salvoravida/react-adal · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/salvoravida/react-adal/pull/115
Improper Authentication in react-adal Snyk	Exploit Third Party Advisory snyk.io text/html	 MISC snyk.io/vuln/SNYK-JS-REACTADAL-1018907

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

[982777](#) Nodejs (npm) Security Update for react-adal (GHSA-7mpx-vg3c-cmr4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	React-adal Project	React-adal	All	All	All	All
Application	React-adal Project	React-adal	All	All	All	All

`cpe:2.3:a:react-adal_project:react-adal:*:*:*:*:node.js:*:*:`

`cpe:2.3:a:react-adal_project:react-adal:*:*:*:*:node.js:*:*:`

Discovery Credit

Kris Hardy

[← 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](#)