Improper Authentication

Affecting react-adal package, versions **<0.5.1**

INTRODUCED: 16 OCT 2020 CVE-2020-7787 CWE-287 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `react-adal` to version 0.5.1 or higher.

Overview

react-adal is an Azure Active Directory Library (ADAL) support for ReactJS.

Affected versions of this package are vulnerable to Improper Authentication. 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.

PoC

```
NOTE: The version number of adal.js in react-adal is marked as 1.0.18, but the file is still vulnerable to the auth bypass
and it does not match v1.0.18 from azure-activedirectory-library-for-js.
```

- `src/adal.js:1106 Vulnerable verification against adal.nonce.idtoken in AuthenticationContext.prototype._matchNonce()`
- `src/adal.js:1125 Vulnerable verification against adal.state.login in AuthenticationContext.prototype._matchState()`
- `src/adal.js:1131-1138 Vulnerable verification against adal.state.renew in AuthenticationContext.prototype._matchState()`

```
A minimal proof-of-concept request template is available in adal_bypass_request.txt (it will require some minor changes for
your test environment), and a minimal JWT token body template is in adal_bypass_jwt.json (it also will require minor
changes). Using a "none" algorithm for generating the JWT token was successful, and using the clientID that can be
retrieved without authentiation from a login redirection to login.microsoftonline.com worked successfully in my tests.

<h3>adal_request_bypass.txt ###</h3> https:///#id_token=&state=&session_state=


<h3>adal_bypass_jwt.json ###</h3> {"aud":"","exp":,"email":"malicious@user.com","name":"Malicious User","nonce":""}
```

References

- GitHub PR

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 8.2 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-REACTADAL-1018907
Published	8 Dec 2020
Disclosed	16 Oct 2020
Credit	Kris Hardy

Report a new vulnerability | Found a mistake?

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.