CIRR_OIDC_AUTH_MODULE Scan Report

Project Name	CIRR_OIDC_AUTH_MODULE
Scan Start	Wednesday, March 11, 2020 12:30:12 AM
Preset	Checkmarx Default
Scan Time	00h:01m:56s
Lines Of Code Scanned	12521
Files Scanned	28
Report Creation Time	Wednesday, March 11, 2020 12:32:14 AM
Online Results	https://cxlilly.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=1091076&projectid=403
Team	Cirrus
Checkmarx Version	8.9.0.210 HF7
Scan Type	Full
Source Origin	LocalPath
Density	8/100000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

Results Limit

Results limit per query was set to 50

Selected Queries

To see the selected queries you must check the 'Executive Summary' option in the 'General' section of the report template

Scan Results Details

Frameable Login Page

Query Path:
Typescript\Cx\Typescript Medium Threat\Frameable Login Page Version:1

Description

Frameable Login Page\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://cxlilly.checkmarx.net/CxWebClient/ViewerMain.aspx?scanid=1091076&projectid=403&pathid=1
Status	Recurrent

The web-application does not properly utilize the "X-FRAME-OPTIONS" header to restrict embedding web-pages inside of a frame.

	Source	Destination
File	src/ensure-login.js	src/ensure-login.js
Line	1	1
Object	X634785337	X634785337

Code Snippet
File Name src/ensure-login.js
Method export default (options) => {

```
....
1.  export default (options) => {
```

Frameable Login Page

Risk

What might happen

Allowing setting of web-pages inside of a frame in an untrusted web-page will leave these web-pages vulnerable to Clickjacking, otherwise known as a redress attack. This may allow an attacker to redress a vulnerable web-page by setting it inside a frame within a malicious web-page. By crafting a convincing malicious web-page, the attacker can then use the overlayed redress to convince the user to click a certain area of the screen, unknowingly clicking inside the frame containing the vulnerable web-page, and thus performing actions within the user's context on the attacker's behalf.

Cause

How does it happen

Failure to utilize the "X-FRAME-OPTIONS" header will likely allow attackers to perform Clickjacking attacks. Properly utilizing the "X-FRAME-OPTIONS" header would indicate to the browser to disallow embedding the web-page within a frame, mitigating this risk, if the browser supports this header. All modern browsers support this header by default.

General Recommendations

How to avoid it

Utilize the "X-FRAME-OPTIONS" header flags according to business requirements to restrict browsers that support this header from allowing embedding web-pages in a frame:

- "X-Frame-Options: DENY" will indicate to the browser to disallow embedding any web-page inside a frame, including the current web-site.
- "X-Frame-Options: SAMEORIGIN" will indicate to the browser to disallow embedding any web-page inside a frame, excluding the current web-site.
- "X-Frame-Options: ALLOW-FROM https://example.com/" will indicate to the browser to disallow embedding any web-page inside a frame, excluding the web-site listed after the ALLOW-FROM parameter.

Source Code Examples

Java

Setting the "DENY" Flag on a Response

```
response.addHeader("X-Frame-Options", "DENY");
```

Scanned Languages

Language	Hash Number	Change Date
JavaScript	1003522720031683	6/2/2019
VbScript	9340222351170833	6/2/2019
Typescript	1488217042171263	6/2/2019
Common	0114668597102001	6/2/2019