

**Finding Name: Vulnerability in AngularJS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | SCR | Project Member | Ontrack | Natalia Khobotova | Yes |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

The OnTrack platform uses AngularJS, which is one of the JavaScript frameworks. The AngularJS version being used is 1.5.11, which is vulnerable to Regular Expression Denial of Service (CVE-2023-26116) and other attacks such as Cross-Site Scripting. Regular Expression Denial of Service is a type of Denial-of-Service attack aimed at making a system inaccessible to its original and legitimate users.

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

If an attacker exploits this vulnerability, they could launch a ReDoS attack on the platform. This could result in the entire web application's services being brought down, as the application would struggle to handle the requests sent by the attacker. This will lead to damage to the business reputation and cause financial losses, as well as the need to invest time and resources to prevent this attack or quickly fix it and resume services once the attack begins.

**Affected Assets**

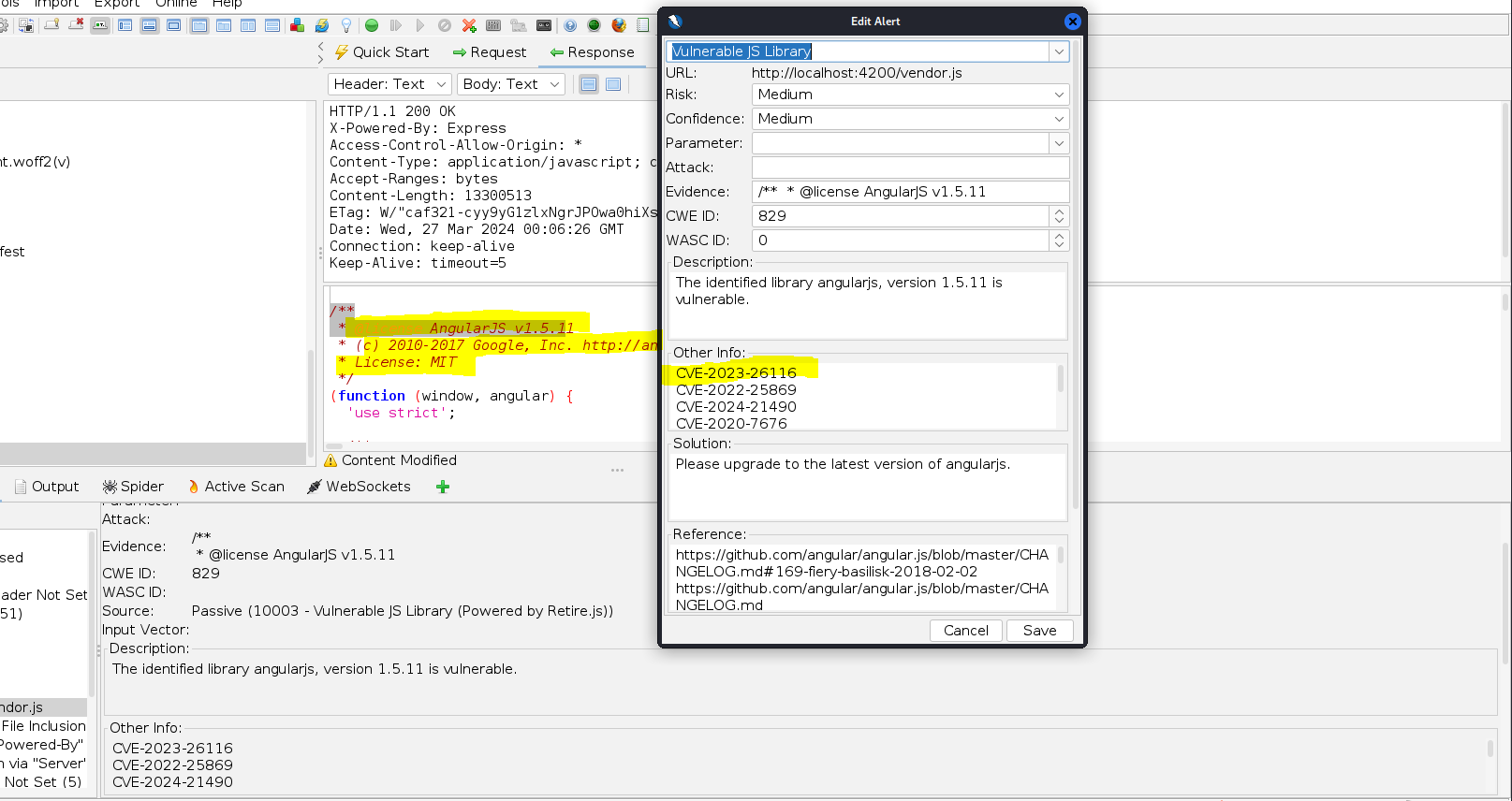
Web application

**Evidence**

Provide a step-by-step guide on how to reproduce the vulnerability with screenshots

**Step 1.**

Check the version of AngularJS, by using OWASP ZAP tool



**Step 2.**

Write script to exploit the vulnerability

A screenshot of a computer program

Description automatically generated

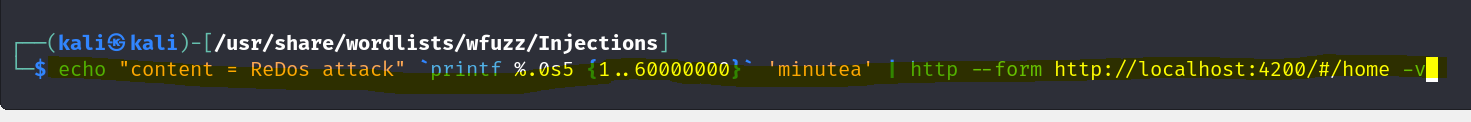
echo "content = ReDos attack" `printf %.0s5 {1..60}` 'minutea' | http --form http://localhost:4200/#/home -v

The script will create regular expressions "{1..60}"

Change '60' to '600000' to send a huge number of regular expressions to the web application.

**Step 3.**

Exploiting the vulnerability caused the application system to go down, preventing users from accessing any unit sites during the attack.



A black and white screen

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

**Remediation Advice**

Update to latest version

**References**

<https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>

<https://www.cybersecurity-help.cz/vdb/SB2023081008>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26116>

OWASP ZAP

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

Great find, Byeongnam. There is much to add or fix. The finding was easily replicated in my environment. However, I had to increase the number of regexes sent, but mentioning this only if someone tries to replicate it in the future.