

**Finding Name: prototype pollution**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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, one of the JavaScript frameworks. The version of AngularJS being used is 1.5.11, which is vulnerable to prototype pollution (CVE-2019-10768). Prototype pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker could manipulate these attributes to overwrite or pollute them. This could lead to various types of attacks, including DoS, remote code execution, and property injection. There are codes that may cause these attacks in the future.

**Risk Rating**  
Impact: Significant  
Likelihood: unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**

This vulnerability could lead to various types of attacks, including DoS, remote code execution, and property injection. These attacks could damage the company's reputation, as they could result in server downtime and data breaches. Businesses could face financial losses as well as the need to invest time and resources to prevent attacks or quickly fix the issue.

**Affected Assets**

Application server

Web server

Web browser

**Evidence**

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

**Step 1.**

**Check the version of Angular JS and discovered that is vulnerable to prototype pollution.**

A screenshot of a computer

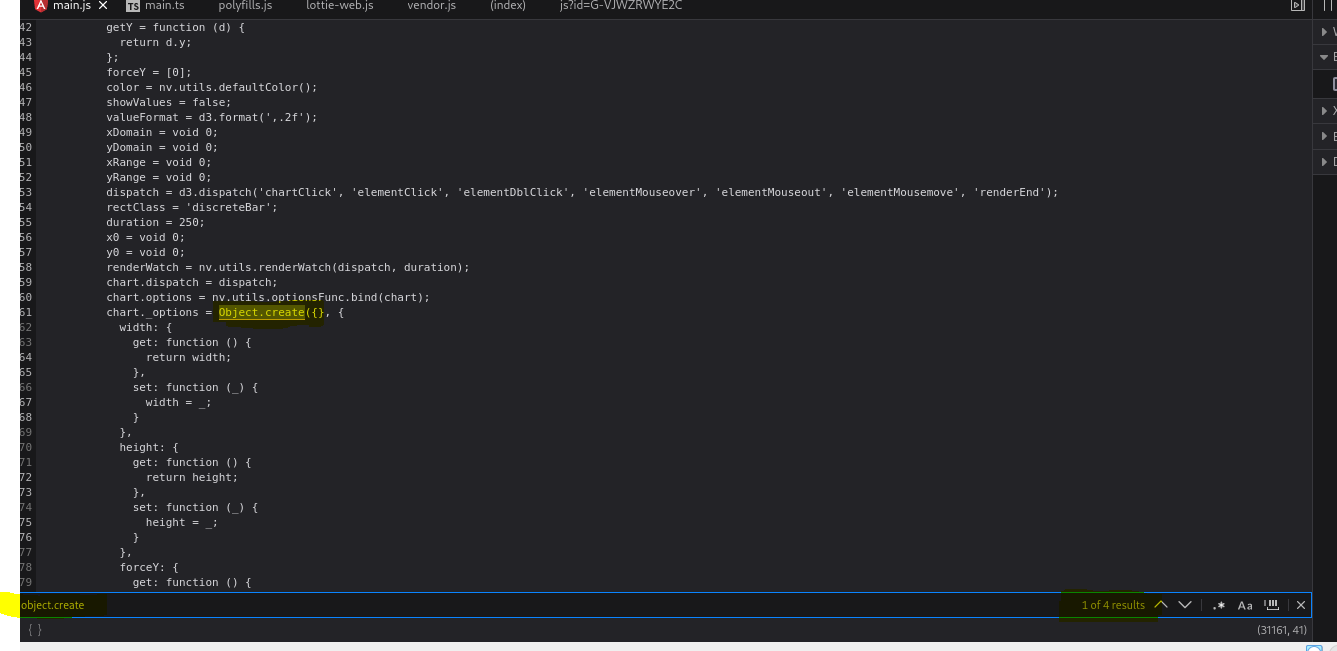
Description automatically generated

**Remediation Advice**

Update Angular JS to latest version

**I've discovered 14 lines of code that use .prototype, which could potentially be exploited. Instead using “.prototype”, freeze the prototype with “object.freeze(object.prototype )”**A screenshot of a computer

Description automatically generated

**When using Object.create(), it's essential to use it with "null", like Object.create(null), to prevent any type of attack. However, I've found four instances where it's used without "null".**

**Using Map instead of Object can indeed mitigate the risk of prototype pollution in this version of AngularJS.**A screenshot of a computer

Description automatically generated

**References**

OWASP ZAP

<https://security.snyk.io/vuln/SNYK-JS-ANGULAR-534884>

<https://portswigger.net/web-security/prototype-pollution>

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

Well written and provides correct impact and likelihood. However, you described remediation in step three in the evidence section, could I please suggest moving it to the remediation advice section? Please also format the document as per your previous finding