

**Finding Name:** Use after free.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | SCR team member | Ontrack | Natalia Khobotova | NO |

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

**Finding Description**

User-after-free (UAF) vulnerabilities happen when a program tries to use memory that's already been freed. It's like throwing something away then trying to hold it. This can crash the program, corrupt data, or even let attackers take control. It occurs in programs that manage their own memory allocation.

**Risk Rating**  
Impact: Significant  
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**

The Use After Free vulnerabilities could lead to severe implications for the business as it could lead to crashing of programs, which could lead to corruption in data of the users leading to loss in trust. Further, the attackers exploit them to steal data or take over systems, halting operations.

**Affected Assets**

The affected assets include the Ontrack website program and server, which could be corrupted in case this type of attack happens.

**Evidence**

The following screenshot shows the line of the vulnerable code:

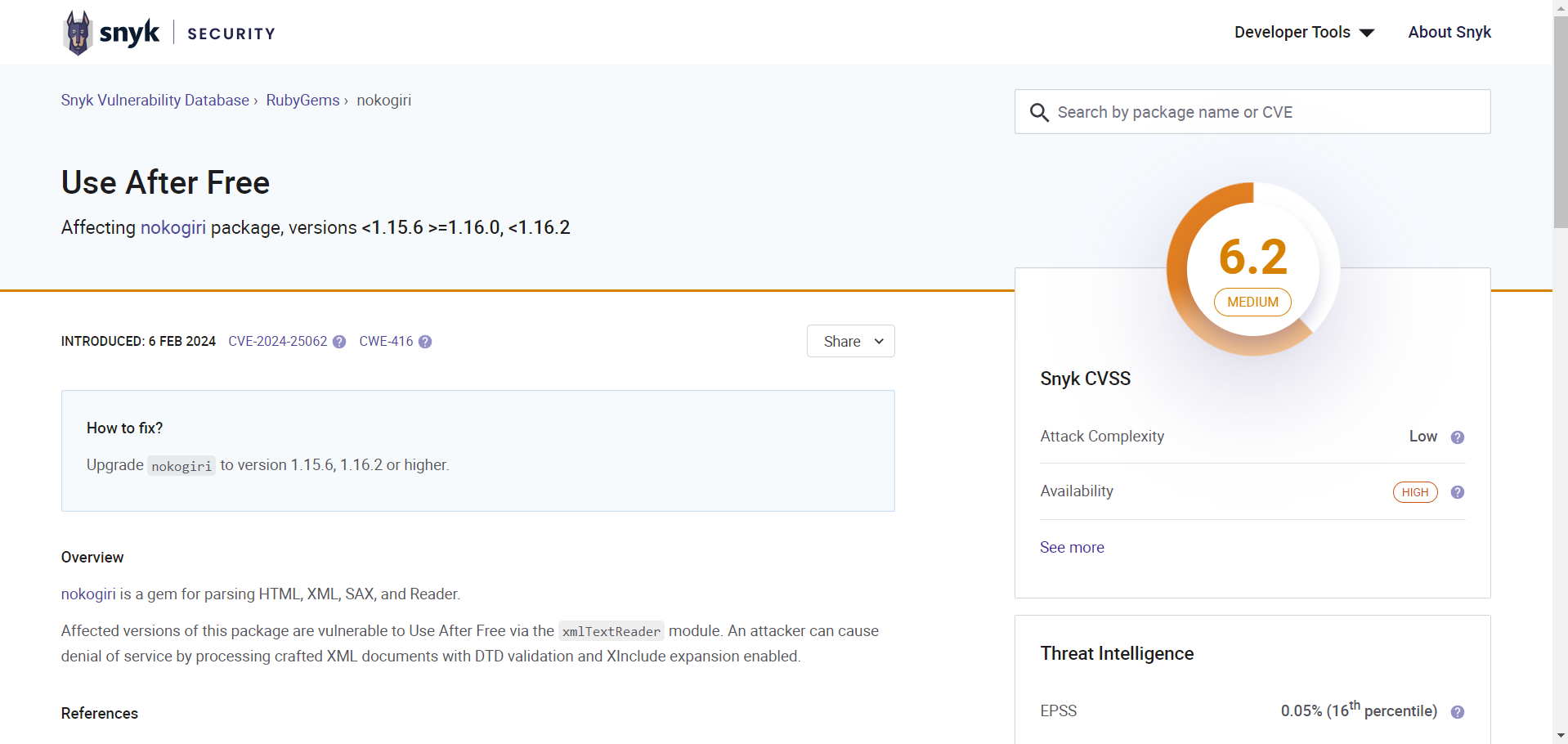
****

**The file is doubtfire-deploy/doubtfire-api/Gemfile.lock.**

****

As it could be seen on line 239, the nokogiri version is 1.14.2, which has the CVE-2024-25062 and the CWE-416 vulnerabilities.

The following screenshots show more details on the same:



**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**

**Remediation Advice**

The vulnerability could be mitigated by upgrading the nokogiri package to version 1.15.6, 1.16.2 or higher.

**References**

[**https://encyclopedia.kaspersky.com/glossary/use-after-free/#:~:text=Use%2DAfter%2DFree%20(UAF,error%20to%20hack%20the%20program**](https://encyclopedia.kaspersky.com/glossary/use-after-free/#:~:text=Use%2DAfter%2DFree%20(UAF,error%20to%20hack%20the%20program)**.**

[**https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-6228056**](https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-6228056)

[**https://cwe.mitre.org/data/definitions/416.html**](https://cwe.mitre.org/data/definitions/416.html)

[**https://www.cve.org/CVERecord?id=CVE-2024-25062**](https://www.cve.org/CVERecord?id=CVE-2024-25062)

**Contact Details**

Gaurish Bhatia

S222187151@deakin.edu.au

**Pentest Leader Feedback.**

Good job!