

**Finding Name:** HTTP Request Smuggling

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | SCR team member | Ontrack | Payas Paul and Jaspriya Kaur | NO |

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

**Finding Description**

HTTP Request Smuggling is a web security exploit that tricks web servers by manipulating how they interpret incoming messages. Imagine a sneaky message with two parts: a harmless looking first half for one server, and a hidden malicious request snuck in later. By exploiting inconsistencies between how different servers (like a firewall and a backend server) read these messages, attackers can potentially bypass security filters or even take control of parts of the system. This vulnerability arises from how certain HTTP headers specify the message length, and it requires careful crafting of requests to target specific server behavior.

**Risk Rating**  
Impact: severe  
Likelihood: certain

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 HTTP Request Smuggling can sneak malicious commands past security, letting attackers steal data, hijack user sessions, or take control of parts of your website. This can cripple operations, damage customer trust, and lead to financial losses.

**Affected Assets**

This assets related to the OnTrack server, which stores the user credentials and data with the functionality of the application.

**Evidence**

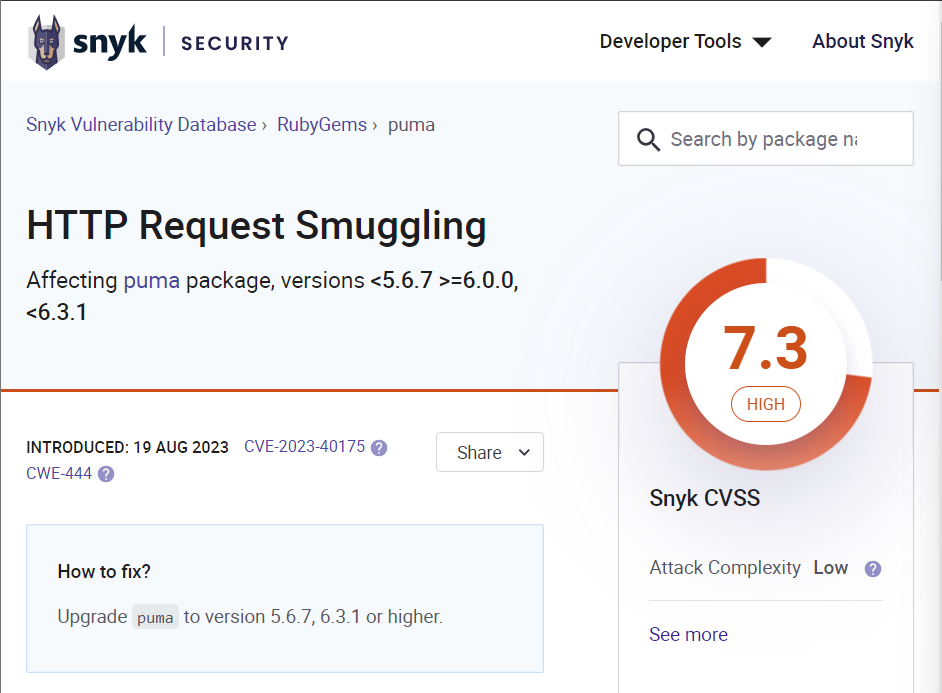
The following screenshot shows the line of the vulnerable code :

**A black screen with white text

Description automatically generated**

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

As it could be seen on line 247, in which the puma version is 6.1.1, which has the CVE-2023-40175 and CWE-444 vulnerabilities.

The details on the same is given in the following screenshots:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Remediation Advice**

The vulnerability could be mitigated by upgrading puma to version 5.6.7, 6.3.1 or higher.

**References**

[**https://security.snyk.io/vuln/SNYK-RUBY-PUMA-5846204**](https://security.snyk.io/vuln/SNYK-RUBY-PUMA-5846204)

[**https://www.cve.org/CVERecord?id=CVE-2023-40175**](https://www.cve.org/CVERecord?id=CVE-2023-40175)

[**https://cwe.mitre.org/data/definitions/444.html**](https://cwe.mitre.org/data/definitions/444.html)

[**https://portswigger.net/web-security/request-smuggling**](https://portswigger.net/web-security/request-smuggling)

**Contact Details**

Gaurish Bhatia

S2221987151@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.