

**Finding Name:** Unencrypted Communications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Mohammad Nouri | PT | Junior Team Member | Ontrack | Nabiha Masood and Oliver Power |  |
|  |  |  |  |  |  |

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

**Finding Description**

Vulnerable Ruby version 3.1.4P

The StringIO gem versions 3.0.1 through 3.0.6 and 3.1.0 through 3.1.4 in Ruby 3.0.x and 3.1.x are vulnerable to a buffer overread issue (CVE-2024-27280). This flaw could allow ungetbyte and ungetc methods to read past the end of a string, potentially exposing memory values. It's recommended to upgrade to StringIO gem version 3.0.1.1 or 3.0.1.2, or utilize StringIO 3.0.3 or later, or Ruby 3.2.x and later, to mitigate this vulnerability.

**Risk Rating**  
Impact: Minor  
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**

Data Breach Risk: Since the vulnerability involves buffer overreading, there's a risk of exposing sensitive data stored in memory. If exploited, attackers could gain unauthorized access to this data, compromising the confidentiality of user information or other critical business data.

Reputation Damage: A data breach or security incident resulting from this vulnerability could damage you’re the company’s reputation. Users may lose trust in the company’s ability to protect their data, leading to decreased user confidence, and potential loss of business.

**Affected Assets**

The web application

**Evidence**

Step 1:

Run an Nmap scan:

A screenshot of a computer

Description automatically generated

Step 2:

Visit <http://localhost:3000> and the version of ruby is displayed on the page:

A screenshot of a computer

Description automatically generated

**Remediation Advice**

update the StringIO gem to version 3.0.3 or later.

**References**

<https://www.ruby-lang.org/en/news/2024/03/21/buffer-overread-cve-2024-27280/>

[**https://nmap.org/**](https://nmap.org/)

**Contact Details**

Mohammad Nouri mnouri@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.