

**Finding Name: Uncontrolled Resource Consumption**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Payas Paul | SCR | Senior Lead | Ontrack | Jaspriya k , Natalia K |  |
|  |  |  |  |  |  |

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

**Finding Description- Hashing**

A defect in the DrawOptions\_initialize method in rmdraw.c is the cause of the Uncontrolled Resource Consumption ('Resource Exhaustion') vulnerability in rmagick@5.2.0. An attacker might use this issue to overload memory resources and cause a denial of service.

**Risk Rating**  
Impact: major  
Likelihood: high

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

Denial of Service (DoS) Risk: An attacker may leverage this vulnerability to perform a DoS attack, which would disrupt your services and bar people from utilizing them.

Operational Disruption: If an assault is successful, it may affect your business's capacity to serve clients and handle transactions, which could result in possible financial losses.

Reputation Damage: Service interruptions and outages may harm your company's standing and cause stakeholders and consumers to lose faith in you.

Financial Impact: There could be large financial losses as a result of the attack's mitigation costs, service restoration costs, and possible loss of revenue during the outage.

Regulatory Compliance: Failure to comply with regulatory standards due to a DoS attack resulting from this vulnerability may result in penalties or legal repercussions.

**Affected Assets**

The following assets are impacted by rmagick@5.2.0's Uncontrolled Resource Consumption (or "Resource Exhaustion") vulnerability:

Application Availability: A denial of service (DoS) attack could be caused by the vulnerability, which would impair your application's availability and bar people from using it.

Data Integrity: Although the vulnerability does not directly affect data integrity, a denial-of-service (DoS) attack could prevent your application from operating normally, which could have an impact on the accuracy of the data being processed or saved.

User Experience: A DoS attack may cause services to be unavailable or degraded, which will negatively affect users' ability to utilize your application.

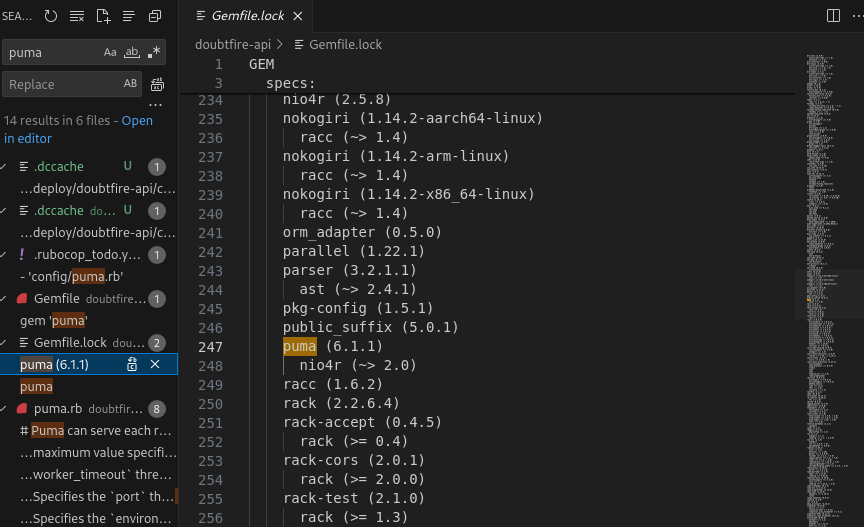
Business Operations: The vulnerability may cause a disturbance in your company's operations, which could affect your capacity to provide customer service, handle payments, and carry out essential tasks.

**Evidence**

**Step 1**

In this case, the vulnerability is doubtfire-deploy/doubtfire-api/Gemfile.Lock line 347

**Step 2.**

****

**Step 3.**

**Remediation Advice**

**Take these actions to rectify the password hashing using MD5:**

Update to rmagick@5.3.0: In order to address the issue and stop unchecked resource consumption, it is imperative that you update to the most recent version of rmagick, which is 5.3.1 or higher.   
Track and Find Abnormalities: Keep an eye on your application's resource utilization to see any odd trends or spikes that might point to a denial-of-service assault.   
Implement Rate limitation: While you upgrade your dependencies, implement rate limitation or other defensive measures to lessen the impact of any denial-of-service attacks.   
Evaluate and Update Dependencies: Make sure all of your project's dependencies are current and free of known vulnerabilities by routinely reviewing and updating them.

**References**

1. **SANS Institute: The SANS Institute offers a wealth of resources on cybersecurity, including articles, training courses, and research papers.** [**SANS Institute**](https://www.sans.org/)
2. **CIS Benchmarks: The Center for Internet Security (CIS) provides benchmarks for securing systems and applications, including specific guidelines for securing web applications. CIS Benchmarks**
3. **Microsoft Security Development Lifecycle (SDL): Microsoft offers guidance on secure software development practices, including recommendations for secure coding and vulnerability mitigation.** [**Microsoft SDL**](https://www.microsoft.com/en-us/securityengineering/sdl)
4. **GitHub Security Lab: GitHub's Security Lab provides resources and tools for improving the security of your software, including guidance on identifying and remediating vulnerabilities.** [**GitHub Security Lab**](https://securitylab.github.com/)

**Contact Details**

Payas Paul (Senor Lead)

[612payaspaul@gmail.com](mailto:612payaspaul@gmail.com)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.