

**Finding Name:** Force SSL

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Gaurish Bhatia | SCR | SCR team member | Ontrack | Jaspriya Kaur and Payas Paul |  |

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

**Finding Description**

This finding indicates a potential lack of encryption in the communication between your application (doubtfire-api) and the server during development. The code snippet shows the configuration file (doubtfire-api/config/environments/development.rb) on line 2, which might be missing the config.force\_ssl setting to enforce HTTPS.

**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**

Unencrypted communication exposes sensitive data (usernames, passwords, etc.) to eavesdropping by attackers. This could lead to breaches, unauthorized access, and compromised accounts. Additionally, it undermines user trust in your application's security practices. This could impact the business as a whole in a devastating way.

**Affected Assets**

* The Doubtfire Api application itself.
* Any data transmitted between the application and the server during development.
* User accounts and credentials potentially exposed due to unencrypted communication.

**Evidence**

The following screenshot shows the line of the vulnerable code :

**A screenshot of a computer

Description automatically generated**

A screen shot of a computer

Description automatically generated

The path is **doubtfire-api/config/environments/development.rb.**

This could be found at the path doubtfire-deploy/doubtfire-api/config/environments/development.rb at the line 2, it could be seen that the algorithm used is less secured and thus it could lead to low encryption.

**Remediation Advice**

Update the **doubtfire-api/config/environments/development.rb** file on line 2 (or the appropriate location) to include **config.force\_ssl = true**. This enforces HTTPS for all communication during development.

Consider using a dedicated development environment with pre-configured security settings to avoid manual configuration errors.

**References**

<https://cwe.mitre.org/data/definitions/757.html>

**Contact Details**

Gaurish Bhatia

S2221987151@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.