A close up of a dragon's face

Description automatically generated

**Finding Name: API Disclosure**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| DEV PATEL | PT | Project Co-lead | EchoNet |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

An API disclosure vulnerability was identified in the application, where sensitive information about the API endpoints and internal implementation details is exposed. This vulnerability occurs when the application fails to adequately restrict access to its API documentation.

**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**

Explain how the finding will impact the company and the application as a whole

**Affected Assets**

Identify assets that are affected by this vulnerability.

**Evidence**

Provide a step-by-step guide on how to reproduce the vulnerability with screenshots

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Remediation Advice**

Provide guidance on how to fix or mitigate the vulnerability.

**References**

Nmap

**Contact Details**

DEV PATEL: - s222622553@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on