#YWH-PGM2713-409 WON'T FIX

/ Information Disclosure on api-app.telenor.se via /api/v1/application.wadl leaks API information

TELENOR SWEDEN PUBLIC BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-07-23

REPORT DETAILS

BUG TYPE	Information Exposure Through Debug Information (CWE-215)
SCOPE	*.telenor.se
ENDPOINT	/api/v1/application.wadl?detail=true , /api/v1/application.wadl
SEVERITY	High
VULNERABLE PART	http-method
PART NAME	/api/v1/application.wadl
PAYLOAD	/api/v1/application.wadl?detail=true
TECHNICAL ENVIRONMENT	Windows 10 , Chrome
APPLICATION FINGERPRINT	
IP USED	45.115.58.138

CVSS SCORE	SEVERITY
7.3	HIGH

VECTOR STRING

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

BUG DESCRIPTION

Exposure of WADL File Containing API Routes and Jersey Endpoint Disclosure on https://api-app.telenor.se/api/v1/application.wadl and https://api-app.telenor.se/api/v1/application.wadl?detail=true

Severity:
Medium

Description:
During a security assessment of the Telenor API application (https://api-app.telenor.se), I identified a potential security vulnerability that allows unauthorized access to sensitive information. The issue involves the exposure of the WSDL (Web Services Description Language) file, which contains API routes and Jersey endpoint details.

Steps to Reproduce:

Navigate to https://api-app.telenor.se/api/v1/application.wadl in a web browser.
The browser displays the content of the WADL file, revealing the API routes and Jersey endpoint information.
Additionally, accessing https://api-app.telenor.se/api/v1/application.wadl?detail=true also displays the sensitive details.

Impact:
The exposure of the WSDL file and Jersey endpoint information can have several adverse consequences, including but not limited to:

Information Disclosure: Unauthorized parties can gain insights into the API structure, potentially identifying weaknesses or security gaps.
Route Manipulation: Attackers could exploit the exposed information to launch targeted attacks on specific API routes, leading to unauthorized access to sensitive data or unauthorized actions.
Security by Obscurity: The WSDL file may contain sensitive implementation details, which could be utilized by attackers to bypass security controls.
Recommendation:
To mitigate this vulnerability and enhance the security of the Telenor API application, I suggest the following actions:

Access Control: Implement access controls on the WSDL file and ensure that only authorized personnel or services can access it.
Endpoint Security: Review the Jersey endpoint configuration and ensure that sensitive information is not inadvertently exposed.
Input Validation and Sanitization: Validate and sanitize user input to prevent any potential exploitation attempts on the exposed API routes.
Secure Coding Practices: Follow secure coding practices to prevent security misconfigurations and information leakage.
API Security Testing: Conduct regular security assessments and penetration testing of the API application to identify and remediate any security weaknesses proactively.

COMMENTS

ADITYASHENDE ON 2023-07-23 10:04:29

NEW

TELENOR SWEDEN ON 2023-07-24 03:16:35

NEW → UNDER REVIEW

Hi ADITYASHENDE,

Thanks for your submission.

Your report will be reviewed by our team and updated in a timely manner.

Regards.

TELENOR SWEDEN ON 2023-07-24 10:09:25

Updated report title.

Exposure of WADL File Containing API Routes and Jersey Endpoint Disclosure → Information Disclosure on api-app.telenor.se via /api/v1/application.wadl leaks API information

TELENOR SWEDEN ON 2023-07-24 10:09:32

UNDER REVIEW → NEED MORE INFO

Hi ADITYASHENDE,

We were able to reproduce the described behavior. However, we are not sure about the security impact of this exploit. We would need more information about the malicious actions that could be taken against the application with the knowledge of these API information.

- **Could you provide us with a PoC that demonstrates an actual security impact through the exploitation of that leakage ?**

If you cannot chain this behavior with any post-exploitation, we wont be able to consider your report as valid, based on our program's non-qualifying vulnerabilities:

- **Disclosure of information without security impact (Stack traces, path disclosure, directory listings, software versions, IP disclosure, 3rd party secrets etc.)**

Thanks for your understanding.

Regards.

TELENOR SWEDEN ON 2023-07-31 12:11:12

Hi ADITYASHENDE,

It's been more than a week since we heard from you.

> / **Could you provide us with a PoC that demonstrates an actual security impact through the exploitation of that leakage ?**

If we don't get a response from you, we'll have to analyze your report as it stands without all demonstrated impact and/or to close your report.

Regards.

TELENOR SWEDEN ON 2023-08-03 10:12:00

NEED MORE INFO → WON'T FIX

Hi,

Thank you for the finding. we do not find this as a security issue and will not fix it.

Regards
Telenor