CryptoGen Nepal

Vulnerability Assessment and Penetration Testing

Urgent Report - II

EST. 2019 - 2022

eSewa Pvt. Ltd.

Summary

The report includes the technical details of our findings during the duration of the Vulnerability Assessment and Penetration Testing. The scope list below is as per the findings presented further in the documentation. The scope mentioned may be vulnerable to vulnerabilities that have not been included in the report and will be assessed further during the project. Any new vulnerabilities will be provided in future update reports and final reports.

Vulnerability List

ID	Vulnerability	Severity	Identified Date	Status
H1	Unauthorized SMS API Access	8.6 (High)	22 June 2022	Not Resolved

Unauthorized SMS API Access	8.6 (High)

Description

The API implemented in the web application is exposed via https://ir-ns.esewa.com.np/api/sms/ce, lacks the authentication mechanism on such. Regarding this vulnerability, the API responsible for delivering text messages was lacking the authentication mechanism.

Impact

An attacker can request the API and send SMS to his/her preferred target imbedding a malicious link for phishing purpose and can also manipulate the customer since the message Is delivered by eSewa official SMS ID.

Recommendation

- Return 404 error for such requests when authentication is missing on it.
- Consider not to expose critical API endpoint in any webpage or source code.

Affected System and endpoint

- https://ir-ns.esewa.com.np/api/sms/ce

Status

Not Remediated

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

Steps for Reproduction

- Enumerate the API endpoint from the web applications.
- Open Postman and Click on Import, Click on Link, enter the URL and press continue.
- Go to api/sms/ce and enter the target Number in the Value and preferred message or link on message value field.
- Click on Send to forward the request.

Evidence

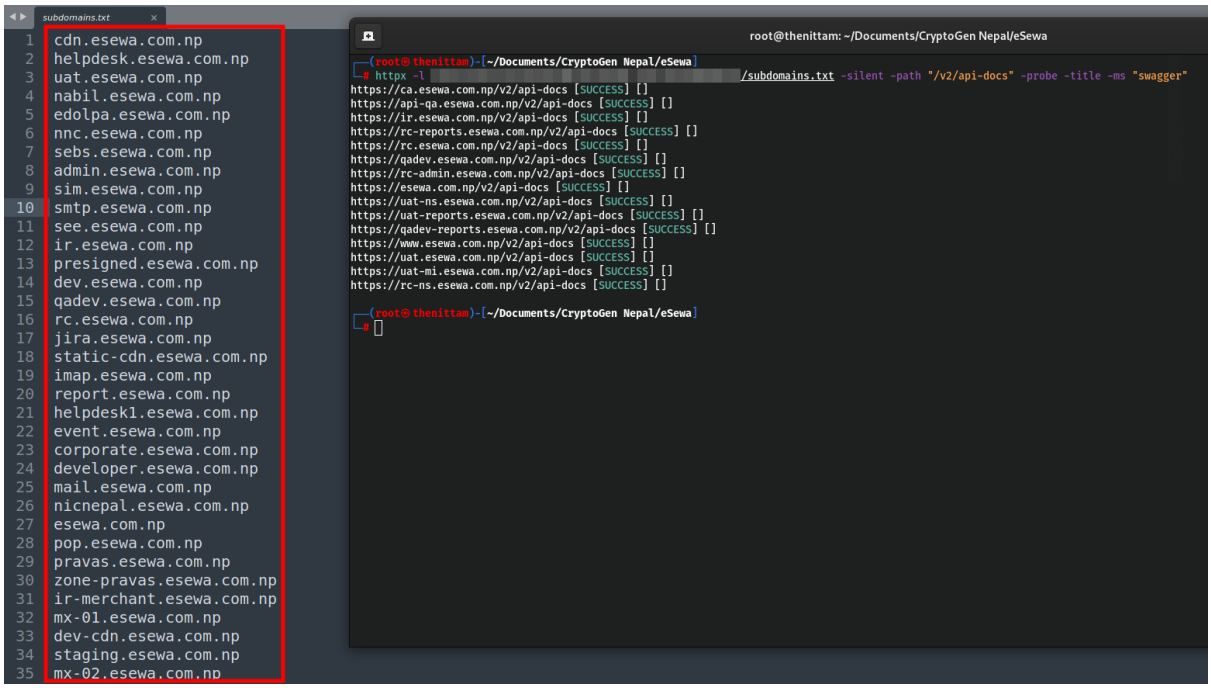

Figure 1 Brute forcing the API endpoints on the subdomains.

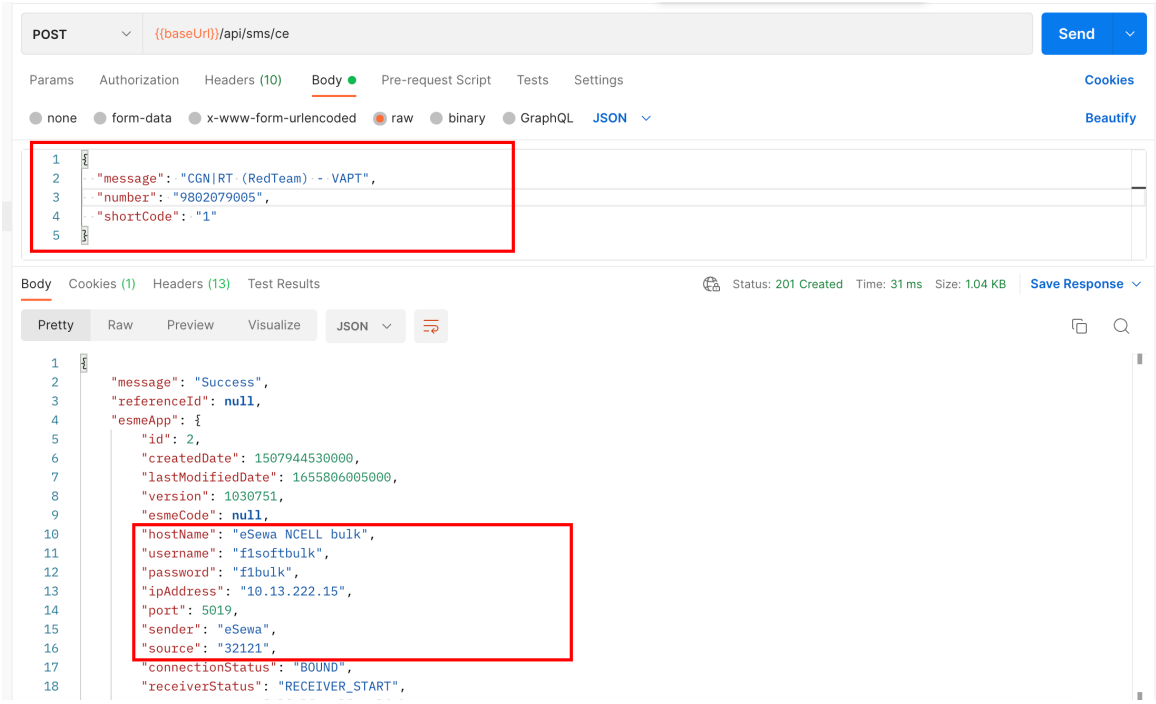

Figure 2 Sending SMS to target number

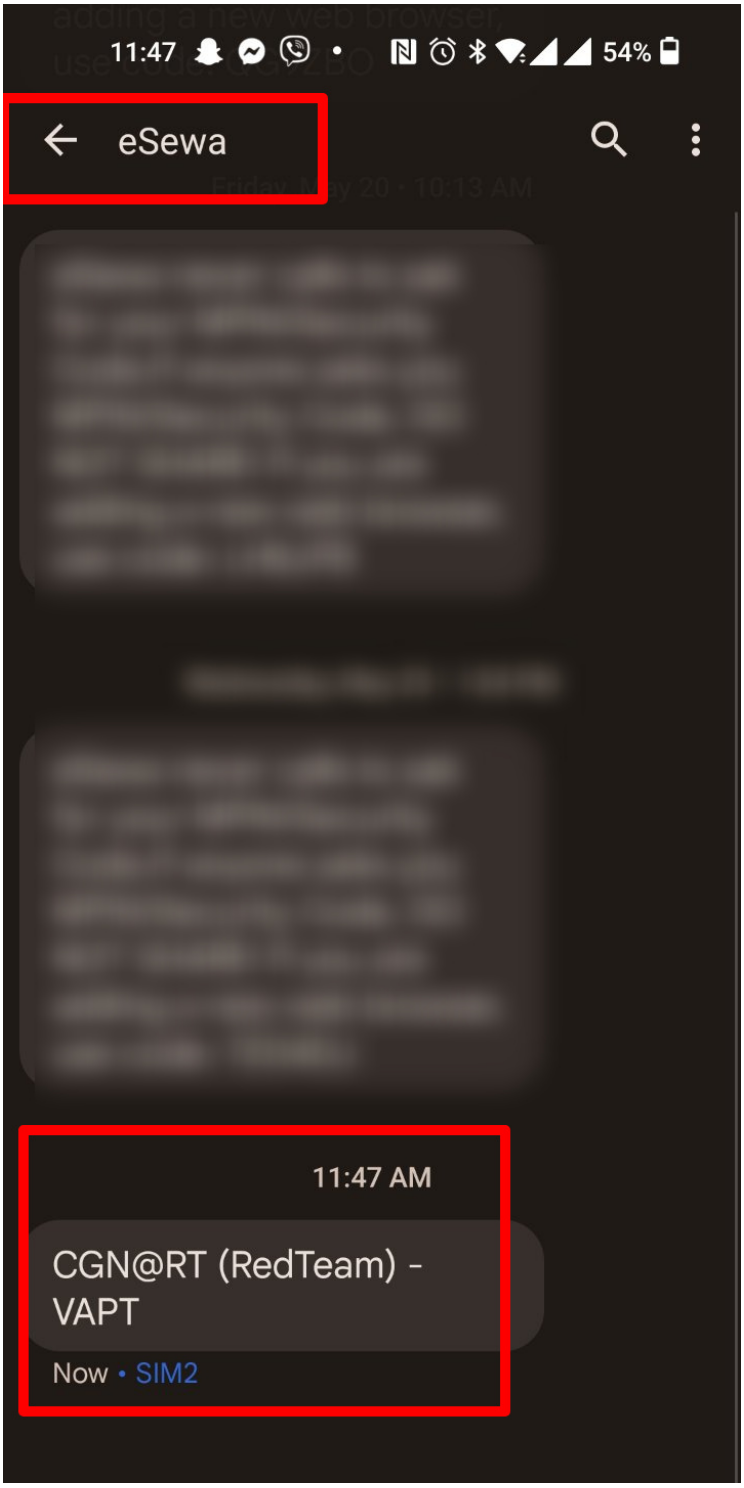

Figure 3 Message received in the target number

References

- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

OUR SERVICES

Our Services As Information Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER CONFIGURATION ASSESSMENT
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

/cryptogennepal
www.cryptogennepal.com
+977-1-4528928
whois@cryptogennepal.com