E-Arogya - Feature #260

Feature # 235 (New): [Security Audit Round 2]

[Security Audit Round 2] OTP Bruteforce (Reapeated)

01/05/2024 12:58 PM - Kalyan Battula

Status:	Closed	**Start date:**	01/05/2024
Priority:	High	**Due date:**	
Assignee:	Kalyan Battula	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

OTP Bruteforce (Repeated)
CWE : CWE-799
Description :
Application allows users to submit multiple wrong OTPs which lead to bruteforce attacks to guess the correct OTP.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
Account takeover can be possible by using this vulnerability.
Evidence/Proof Of Concept :
Step 1: Application accepting multiple OTP requests which leads to brute force the OTP by submitting multiple requests.
clipboard-202405011257-kqohn.png

Step 2: Functionalilty issue
clipboard-202405011258-j6kit.png

Recommendation :
It is recommended to allow only 3 to 5 wrong attempts of OTPs. After the limit block the mobile number for some time or provide a new OTP.

History

#1 - 03/05/2024 04:48 AM - Harish Beechani

- Status changed from New to Resolved

#2 - 03/05/2024 05:23 AM - Sivakanth Kesiraju

- Target version set to Sprint 1 (29th April - 3rd May)

#3 - 03/05/2024 05:27 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

#4 - 10/05/2024 06:18 AM - Harish Beechani

- Assignee set to Harish Beechani

#5 - 10/05/2024 07:17 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

#6 - 16/05/2024 04:51 AM - Kalyan Battula

- Status changed from Ready for Prod to Closed

- Assignee changed from Harish Beechani to Kalyan Battula

working fine now not allowing multiple Opt attempts

Files

clipboard-202405011257-kqohn.png	47 KB	01/05/2024	Kalyan Battula
clipboard-202405011258-j6kit.png	430 KB	01/05/2024	Kalyan Battula