E-Arogya - Feature #256

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

[Security Audit Round 2] Improper Session Management / Session Expiration too longer (Repeated)

01/05/2024 12:53 PM - Kalyan Battula

Status:	Ready for Prod	**Start date:**	01/05/2024
Priority:	High	**Due date:**	
Assignee:	Harish Beechani	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

Improper Session Management / Session Expiration too longer (Repeated)
observation : Repeated
CWE : CWE-613
Description :
In this application a single fixed token is in use for single user, token expiry time also
too longer.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
It helps the attackers to submit without any authentication.
Evidence/Proof Of Concept :
Step 1: Login to the application with any user.And Capture the request.Here application
using the JWT token for user token as shown as below screenshot.
clipboard-202405011252-t5xtj.png

Step 2: Now, observe the expiration token of the JWT token. It is noticed that expiration time
of the token was too long as shown in below screenshot.
clipboard-202405011252-64u3c.png

Recommendation :
It is recommended to maintain session id after login and destroy it after logout.
Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_
Cheat_Sheet.htm

History

#1 - 02/05/2024 09:33 PM - Vasudev Mamidi

- Assignee set to Harish Beechani

#2 - 03/05/2024 05:27 AM - Sivakanth Kesiraju

- Target version set to Security Audit

#3 - 10/05/2024 06:14 AM - Harish Beechani

- Status changed from New to Resolved

#4 - 10/05/2024 07:16 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

Files

clipboard-202405011252-t5xtj.png	107 KB	01/05/2024	Kalyan Battula
clipboard-202405011252-64u3c.png	88.9 KB	01/05/2024	Kalyan Battula