

E-Arogya - Bug #95

Feature # 65 (New): Security Audit

[Security Audit] 30- Port misconfiguration

17/04/2024 04:14 PM - Kalyan Battula

Status:	Closed	Start date:	17/04/2024
Priority:	Low	Due date:	
Assignee:	Uday Kumar Dara	% Done:	0%
Category:		Estimated time:	0:00 hour
Target version:	Security Audit	Spent time:	0:00 hour
Deployed In:		Category:	
Description 30 -Port misconfiguration CWE : CWE-16 Description : During the security audit it was observed that the application is configured on different ports such as http (80) and https (443) Affected Path(s) : https://earogya.satragroup.in/http://earogya.satragroup.in/ *-Applicable to entire application Impact : If the application is using cleartext transmission protocols then there are possibilities of MITM attacks. Recommendation : It is recommended to use only secure communication protocols for data transmission. Evidence/Proof Of Concept : Step 1: Application hosted on both http (80) and https (443) ports. clipboard-202404171614-zny62.png Step 2: Application hosted on both http (80) and https (443) ports. clipboard-202404171614-wcf2v.png			

History

- #1 - 25/04/2024 11:47 PM - Vasudev Mamidi
- Status changed from New to Resolved
- #2 - 26/04/2024 12:01 AM - Vasudev Mamidi
- Assignee set to Uday Kumar Dara
- #3 - 03/05/2024 05:23 AM - Sivakanth Kesiraju
- Target version set to Sprint 1 (29th April - 3rd May)
- #4 - 03/05/2024 05:27 AM - Sivakanth Kesiraju
- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit
- #5 - 30/09/2024 04:34 PM - Gautam Kumar
- Status changed from Resolved to Closed

Files

clipboard-202404171614-zny62.png	520 KB	17/04/2024	Kalyan Battula
clipboard-202404171614-wcf2v.png	114 KB	17/04/2024	Kalyan Battula