

E-Arogya - Feature #286

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

[Security Audit Round 2 ] Port misconfiguration (Repeated)

01/05/2024 01:23 PM - Kalyan Battula

<b>Status:</b>	Ready for Prod	<b>Start date:</b>	01/05/2024
<b>Priority:</b>	High	<b>Due date:</b>	
<b>Assignee:</b>	Uday Kumar Dara	<b>% Done:</b>	0%
<b>Category:</b>		<b>Estimated time:</b>	0:00 hour
<b>Target version:</b>	Security Audit	<b>Spent time:</b>	0:00 hour
<b>Deployed In:</b>		<b>Category:</b>	
<b>Description</b> Port misconfiguration (Repeated) 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) : <a href="https://earogya.satragroup.in/http://earogya.satragroup.in/">https://earogya.satragroup.in/http://earogya.satragroup.in/</a> *-Applicable to entire application Impact : If the application is using cleartext transmission protocols then there are possibilities of MITM attacks. Evidence/Proof Of Concept : Step 1: Application hosted on both http (80) and https (443) ports. clipboard-202405011323-bcoah.png  Step 2: Application hosted on both http (80) and https (443) ports. clipboard-202405011323-ddq7o.png  Recommendation : It is recommended to use only secure communication protocols for data transmission.			

History

- #1 - 02/05/2024 09:14 PM - Vasudev Mamidi  
- Assignee set to Uday Kumar Dara
- #2 - 03/05/2024 04:16 AM - Harish Beechani  
- Status changed from New to Resolved
- #3 - 03/05/2024 05:23 AM - Sivakanth Kesiraju  
- Target version set to Sprint 1 (29th April - 3rd May)
- #4 - 03/05/2024 05:28 AM - Sivakanth Kesiraju  
- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit
- #5 - 10/05/2024 07:19 AM - Harish Beechani  
- Status changed from Resolved to Ready for Prod

Files

clipboard-202405011323-bcoah.png	462 KB	01/05/2024	Kalyan Battula
clipboard-202405011323-ddq7o.png	83 KB	01/05/2024	Kalyan Battula