E-Arogya - Feature #263

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

[Security Audit Round 2] Client side bypass / Improper server side validation

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

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

Description

Client side bypass / Improper server side validation
CWE : CWE-602
Description :
The software is composed of a server that relies on the client to implement a mechanism that is intended to protect the server.
Affected Path(s) :
https://his-user-management-service.satragroup.in/master/user-profile *-Applicable to entire application
Impact :
When the server relies on protection mechanisms placed on the client side, an attacker can modify the client-side behavior to bypass the protection mechanisms resulting in potentially unexpected interactions between the client and server. The consequences will vary, depending on what the mechanisms are trying to protect.
Evidence/Proof Of Concept :
Step 1: Login to the application with test1_fd credentials and navigate to the users under the Masterdata dropdown.Here service entity is disable as shown in below screenshot.
clipboard-202405011300-ouaso.png

Step 2: Capture the above request and modify the value as depicted in the screenshot below. Observe Resource has been created successfully.
clipboard-202405011301-g8kwy.png

Recommendation :
It is recommended to validate the user input at server side. It is recommended to enforce an application URL space white list and implement proper access control.

History

#1 - 03/05/2024 05:27 AM - Sivakanth Kesiraju

- Target version set to Security Audit

#2 - 10/05/2024 06:15 AM - Harish Beechani

- Status changed from New to Resolved

#3 - 10/05/2024 07:17 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

Files

clipboard-202405011300-ouaso.png	80.2 KB	01/05/2024	Kalyan Battula
clipboard-202405011301-g8kwy.png	76.4 KB	01/05/2024	Kalyan Battula