E-Arogya - Feature #241

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

[Security Audit Round 2] Password Returned in Response

01/05/2024 12:27 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

Password Returned in Response
observation : New
CWE : CWE_204
Description :
Some applications return passwords submitted to the application in clear form in later responses. This behavior increases the risk that users' passwords will be captured by an attacker.
Affected Path(s) :
https://his-user-management-service.satragroup.in/master/user-profile *-Applicable to entire application
Impact :
Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.
Evidence/Proof Of Concept :
Step 1: Password Returned in Response as shown in below screenshot
clipboard-202405011227-ei7ou.png

Recommendation :
It is recommended not to disclose passwords in later response.

History

#1 - 02/05/2024 09:36 PM - Vasudev Mamidi

- Assignee set to Harish Beechani

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

- Target version set to Security Audit

#3 - 03/05/2024 05:52 AM - Harish Beechani

- Status changed from New to Resolved

#4 - 10/05/2024 07:15 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

#5 - 16/05/2024 05:08 AM - Kalyan Battula

- Status changed from Ready for Prod to Closed

- Assignee changed from Harish Beechani to Kalyan Battula

Files

clipboard-202405011227-ei7ou.png	83.3 KB	01/05/2024	Kalyan Battula