E-Arogya - Bug #73

Feature # 65 (New): Security Audit

[Security Audit] 8- Insecure Direct Object Reference (IDOR)

17/04/2024 03:43 PM - Kalyan Battula

Status:	Closed	**Start date:**	17/04/2024
Priority:	High	**Due date:**	
Assignee:	Vasudev Mamidi	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

8- Insecure Direct Object Reference (IDOR)

CWE : CWE-639
Description :
An indirect object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which allows attackers to manipulate these references to access unauthorized data.
Affected Path(s) :
https://his-healthid-service.satragroup.in/abdm/search/searchByHealthId *-Applicable to entire application
Impact :
Such flaws can compromise all the data that can be referenced by the parameter. Unless object references are unpredictable, it's easy for an attacker to access all available data of that type.
Recommendation :
Use per user or session indirect object references. This prevents attackers from directly targeting unauthorized resources.
Check access. Each use of a direct object reference from an untrusted source must include an access control check to ensure the user is authorized for the requested object
Evidence/Proof Of Concept :
Step 1: Login to the application with srinuks.1(abha login) credentials and natigate the https://his-healthid-service.satragroup.in/abdm/search/searchByHealthId url and capture the request with a certain "Health ID" as shown in below screenshot.
clipboard-202404171542-1lnzg.png

Step 2: Now Modify the Health ID srinuks.1 to thisiskarthik and forward the request, in the response it can be observed that the data of a different user can be accessed.
clipboard-202404171543-tinfk.png

History

#1 - 24/04/2024 12:39 AM - Vasudev Mamidi

- Assignee set to Vasudev Mamidi

#2 - 24/04/2024 12:53 AM - Vasudev Mamidi

- Status changed from New to In Progress

#3 - 02/05/2024 09:41 PM - Vasudev Mamidi

- Status changed from In Progress to Resolved

#4 - 03/05/2024 05:24 AM - Sivakanth Kesiraju

- Target version set to Sprint 1 (29th April - 3rd May)

#5 - 03/05/2024 05:28 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

#6 - 30/09/2024 05:22 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171542-1lnzg.png	79.1 KB	17/04/2024	Kalyan Battula
clipboard-202404171543-tinfk.png	69.8 KB	17/04/2024	Kalyan Battula