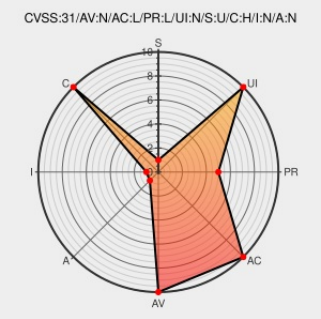
CVE-2021-40375

Published on: Not Yet Published

Last Modified on: 04/13/2022 03:02:00 PM UTC

CVE-2021-40375

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openeyes from Apperta contain the following vulnerability:

Apperta Foundation OpenEyes 3.5.1 allows remote attackers to view the sensitive information of patients without having the intended level of privilege. Despite OpenEyes returning a Forbidden error message, the contents of a patient's profile are still returned in the server response. This response can be read in an intercepting proxy or by viewing the page source. Sensitive information returned in responses includes patient PII and medication records or history.

CVE-2021-40375 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GitHub - DCKanto/CVE-2021-40375		MISC github.com/DCKanto/CVE-2021-40375

GitHub - DCKento/CVE-2021-40375	github.com text/html	MISC github.com/DCKento/CVE-2021-40375
OpenEyes™	openeyes.apperta.org text/html	MISC openeyes.apperta.org/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apperta	Openeyes	3.5.1	All	All	All

cpe:2.3:a:apperta:openeyes:3.5.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@marcus_baw	@AppertaUK you have XSS and privilege escalation vulns in OpenEyes 3.5.1.... github.com/DCKento/CVE-20… github.com/DCKento/CVE-20…	2021-10-30 10:54:21
@robdykedotcom	github.com/DCKento/CVE-20…	2021-10-30 11:24:13
@CVEreport	CVE-2021-40375 : Apperta Foundation OpenEyes 3.5.1 allows remote attackers to view the sensitive information of pat… twitter.com/i/web/status/1…	2022-04-06 02:04:54
/r/netcve	CVE-2021-40375	2022-04-06 02:38:54

← Previous ID

Next ID→