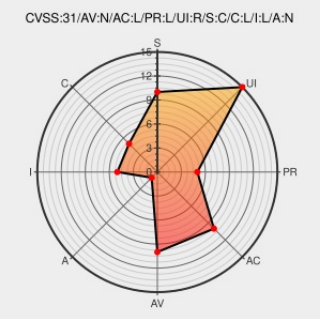
CVE-2021-40374

Published on: Not Yet Published

Last Modified on: 04/12/2022 07:22:00 PM UTC

CVE-2021-40374

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



Certain versions of Openeye from Apperta contain the following vulnerability:

A stored cross-site scripting (XSS) vulnerability was identified in Apperta Foundation OpenEyes 3.5.1. Updating a patient's details allows remote attackers to inject arbitrary web script or HTML via the Address1 parameter. This JavaScript then executes when the patient profile is loaded, which could be used in a XSS attack.

CVE-2021-40374 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
GitHub - DCKento/CVE-2021-40374: XSS	github.com text/html	MISC github.com/DCKento/CVE-2021-40374
OpenEyes™	openeyes.apperta.org	MISC openeyes.apperta.org/

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	Openeye	3.5.1	All	All	All

cpe:2.3:a:apperta:openeye: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
@CVEreport	CVE-2021-40374 : A stored cross-site scripting #XSS vulnerability was identified in Apperta Foundation OpenEyes 3… twitter.com/i/web/status/1…	2022-04-06 02:04:28
/r/netcve	CVE-2021-40374	2022-04-06 02:38:53

← Previous ID Next ID→