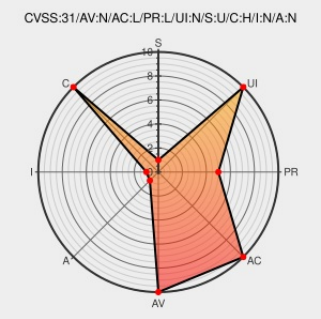
CVE-2020-26564

Published on: 07/31/2021 12:00:00 AM UTC

Last Modified on: 08/09/2021 06:58:00 PM UTC

CVE-2020-26564

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



Certain versions of Opinio from Objectplanet contain the following vulnerability:

ObjectPlanet Opinio before 7.15 allows XXE attacks via three steps: modify a .css file to have <!ENTITY content, create a .xml file for a generic survey template (containing a link to this .css file), and import this .xml file at the survey/admin/folderSurvey.do?action=viewImportSurvey['importFile'] URI. The XXE can then be triggered at a admin/preview.do?action=previewSurvey&surveyId= URI.

CVE-2020-26564 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
ObjectPlanet Opinio 7.13 / 7.14 XML Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163707/ObjectPlanet-Opinio-7.13-7.14-XML-Injection.html

Opinio changes	www.objectplanet.com text/html	CONFIRM www.objectplanet.com/opinio/changelog.html

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	Objectplanet	Opinio	All	All	All	All

cpe:2.3:a:objectplanet:opinio:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-26564 : ObjectPlanet Opinio before 7.15 allows XXE attacks via three steps: modify a .css file to have <!E… twitter.com/i/web/status/1…	2021-07-31 17:04:41

← Previous ID

Next ID→