



CVE-2021-27940

Published on: 03/03/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:48 PM UTC

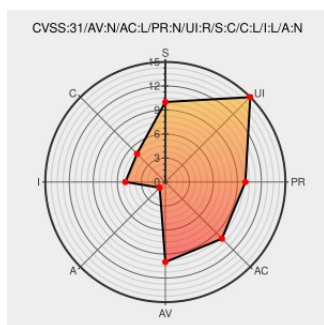
CVE-2021-27940

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Orchestrator](#) from [Openark](#) contain the following vulnerability:

resources/public/js/orchestrator.js in openark orchestrator before 3.2.4 allows XSS via the orchestrator-msg parameter.

CVE-2021-27940 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Orchestrator XSS CVE-2021-27940 - YouTube	Exploit Third Party Advisory www.youtube.com text/html	MISC www.youtube.com/watch?v=DOYm0DIS3Us

Release GA release v3.2.4 · openark/orchestrator · GitHub

Release Notes

Third Party Advisory

github.com

text/html

MISC

github.com/openark/orchestrator/releases/tag/v3.2.4

XSS: sanitize 'orchestrator-msg' param by shlomi-noach · Pull Request #1313 · openark/orchestrator · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/openark/orchestrator/pull/1313

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	Openark	Orchestrator	All	All	All	All
Application	Openark	Orchestrator	All	All	All	All

cpe:2.3:a:openark:orchestrator:*.***.***.***:

cpe:2.3:a:openark:orchestrator:*.***.***.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →