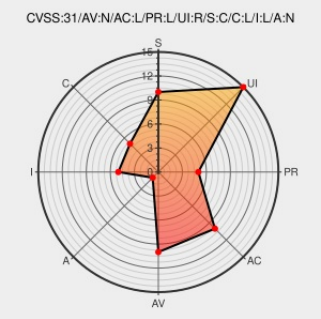
CVE-2022-25224

Published on: Not Yet Published

Last Modified on: 05/31/2022 03:33:00 PM UTC

CVE-2022-25224

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



Certain versions of Proton from Proton Project contain the following vulnerability:

Proton v0.2.0 allows an attacker to create a malicious link inside a markdown file. When the victim clicks the link, the application opens the site in the current frame allowing an attacker to host JavaScript code in the malicious link in order to trigger an XSS attack. The 'nodeIntegration' configuration is set to on which allows the 'webpage' to use 'NodeJs' features, an attacker can leverage this to run OS commands.

CVE-2022-25224 has been assigned by help@fluidattacks.com 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
Proton v0.2.0 - XSS To RCE | Fluid Attacks	fluidattacks.com text/html	MISC fluidattacks.com/advisories/lennon/

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	Proton Project	Proton	0.2.0	All	All	All

cpe:2.3:a:proton_project:proton:0.2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-25224 : Proton v0.2.0 allows an attacker to create a malicious link inside a markdown file. When the victi… twitter.com/i/web/status/1…	2022-05-20 12:08:37
@LinInfoSec	Nodejs - CVE-2022-25224: fluidattacks.com/advisories/len…	2022-05-20 15:00:18
/r/netcve	CVE-2022-25224	2022-05-20 12:38:58

← Previous ID

Next ID→