



CVE-2019-16763

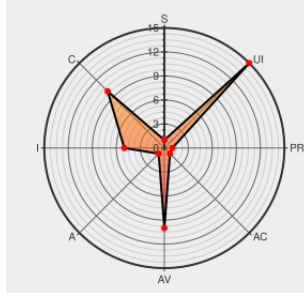
Published on: 11/22/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16763 - advisory for GHSA-m52x-29pq-w3vv

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:N



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

In Pannellum from 2.5.0 through 2.5.4 URLs were not sanitized for data URIs (or vbscript:), allowing for potential XSS attacks. Such an attack would require a user to click on a hot spot to execute and would require an attacker-provided configuration. The most plausible potential attack would be if pannellum.htm was hosted on a domain that shared

cookies with the targeted site's user authentication; an `<iframe>` could then be embedded on the attacker's site using pannellum.htm from the targeted site, which would allow the attacker to potentially access information from the targeted site as the authenticated user (or worse if the targeted site did not have adequate CSRF protections) if the user clicked on a hot spot in the attacker's embedded panorama viewer. This was patched in version 2.5.5.

CVE-2019-16763 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: mpretroff - pannellum version = 2.5.0

Affected Vendor/Software: mpretroff - pannellum version = 2.5.1

Affected Vendor/Software: mpretroff - pannellum version = 2.5.2

Affected Vendor/Software: mpretroff - pannellum version = 2.5.3

Affected Vendor/Software: mpretroff - pannellum version = 2.5.4

Vulnerability Patch/Work Around

Don't host pannellum.htm on a domain that shares cookies with user authentication.

CVSS3 Score: **6.1 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK

LOW

NONE

REQUIRED

NETWORK	LOW	NONE	RESOLVED
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
XSS vulnerability · Advisory · mpetroff/pannellum · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/mpetroff/pannellum/security/advisories/GHSA-m52x-29pq-w3vv
Merge pull request from GHSA-m52x-29pq-w3vv · mpetroff/pannellum@cc2f3d9 · GitHub	Patch github.com text/html	MISC github.com/mpetroff/pannellum/commit/cc2f3d99953de59db908e0c6efd1c2c17f7c6914

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.

Related QID Numbers

983998 Nodejs (npm) Security Update for pannellum (GHSA-m52x-29pq-w3vv)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pannellum	Pannellum	All	All	All	All
cpe:2.3:a:pannellum:pannellum:*:*:*:*:*:						

Discovery Credit

Thank you to Max Schaefer of GitHub Security Lab for reporting this issue.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)