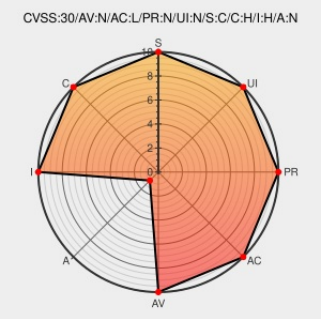
CVE-2019-13020

Published on: 08/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

CVE-2019-13020

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



Certain versions of Tightrope Media Carousel from Trms contain the following vulnerability:

The fetch API in Tightrope Media Carousel before 7.1.3 has CarouselAPI/v0/fetch?url= SSRF. This has two potential areas for abuse. First, a specially crafted URL could be used in a phishing attack to hijack the trust the user and the browser have with the website and could serve malicious content from a third-party attacker-controlled system. Second, arguably more severe, is the potential for an attacker to circumvent firewall controls, by proxying traffic, unauthenticated, into the internal network from the internet.

CVE-2019-13020 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 10 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Carousel Digital Signage - Carousel	Release Notes	CONFIRM www.carouselsignage.com/release_notes/carousel_7

Carousel Digital Signage - Carousel 7.1.3	Release Notes web.archive.org text/html Inactive Link Not Archived	CONFIRM www.carouselsignage.com/release-notes/carousel-7-1-3

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	Trms	Tightrope Media Carousel	All	All	All	All
Application	Trms	Tightrope Media Carousel	All	All	All	All

cpe:2.3:a:trms:tightrope_media_carousel:*:*:*:*:*:*:*:*:

cpe:2.3:a:trms:tightrope_media_carousel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→