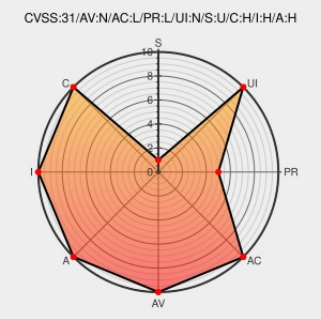
CVE-2018-18931

Published on: 10/29/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18931

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



Certain versions of Carousel Digital Signage from Trms contain the following vulnerability:

An issue was discovered in the Tightrope Media Carousel digital signage product 7.0.4.104. Due to insecure default permissions on the C:\TRMS\Services directory, an attacker who has gained access to the system can elevate their privileges from a restricted account to full SYSTEM by replacing the Carousel.Service.exe file with a custom malicious executable. This service is independent of the associated IIS web site, which means that this service can be manipulated by an attacker without losing access to vulnerabilities in the web interface (which would potentially be used in conjunction with this attack, to control the service). Once the attacker has replaced Carousel.Service.exe, the server can be restarted using the command "shutdown -r -t 0" from a web shell, causing the system to reboot and launching the malicious Carousel.Service.exe as SYSTEM on startup. If this malicious Carousel.Service.exe is configured to launch a reverse shell back to the attacker, then upon reboot the attacker will have a fully privileged remote command-line environment to manipulate the system further.

CVE-2018-18931 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Vulnerabilities in Tightrope Media Systems Carousel – DrewGreen.net	Exploit Third Party Advisory www.drewgreen.net text/html	MISC www.drewgreen.net/vulnerabilities-in-tightrope-media-systems-carousel/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trms	Carousel Digital Signage	All	All	All	All

cpe:2.3:a:trms:carousel_digital_signage:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→