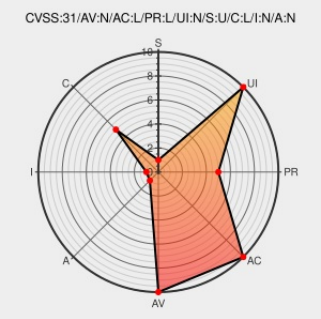
CVE-2019-20354

Published on: 01/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20354

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



Certain versions of Pisignage from Pisignage contain the following vulnerability:

The web application component of piSignage before 2.6.4 allows a remote attacker (authenticated as a low-privilege user) to download arbitrary files from the Raspberry Pi via api/settings/log?file=../ path traversal. In other words, this issue is in the player API for log download.

CVE-2019-20354 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
piSignage/RELEASE NOTES.md at master · colloqi/piSignage · GitHub	Release Notes github.com text/html	MISC github.com/colloqi/piSignage/blob/master/RELEASE%20NOTES.md

Path Traversal vulnerability · Issue #97 · colloqi/piSignage · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/colloqi/piSignage/issues/97
piSignage 2.6.4 Directory Traversal ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155864/piSignage-2.6.4-Directory-Traversal.html

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	Pisignage	Pisignage	All	All	All	All
Application	Pisignage	Pisignage	All	All	All	All

cpe:2.3:a:pisignage:pisignage:*:*:*:*:*:*:*:*:

cpe:2.3:a:pisignage:pisignage:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→