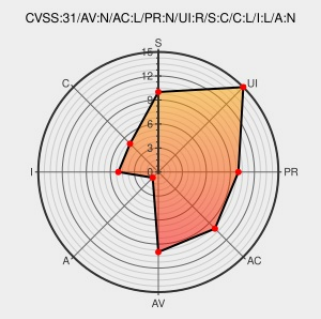
CVE-2019-19736

Published on: 12/30/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:07:00 AM UTC

CVE-2019-19736

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



Certain versions of Yetishare from Mfscripts contain the following vulnerability:

MFScripts YetiShare 3.5.2 through 4.5.3 does not set the HttpOnly flag on session cookies, allowing the cookie to be read by script, which can potentially be used by attackers to obtain the cookie via cross-site scripting.

CVE-2019-19736 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
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
YetiShare 3.5.2–4.5.3, Multiple vulnerabilities | by Jinny Ramsmark | Medium	medium.com text/html	MISC medium.com/@jra8908/yetishare-3-5-2-4-5-3-multiple-vulnerabilities-2d01d0cd7459

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	Mfscripts	Yetishare	All	All	All	All

cpe:2.3:a:mfscripts:yetishare:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report