



CVE-2019-20059

Published on: 02/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-20059

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

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

payment_manage.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.4 directly insert values from the sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection. NOTE: this issue exists because of an incomplete fix for CVE-2019-19732.

CVE-2019-20059 has been assigned by [M](#) 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	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
MFScripts - Full PHP Site Scripts - Ready To Go Professional Websites	Product mfscripts.com	MISC mfscripts.com/

[text/html](#)

GitHub - jra89/CVE-2019-20059: Yetishare SQL Injection in sSortDir_0 parameter - v3.5.2 - v4.5.4. Apart from an admin being able to exploit this, it could also be used in a CSRF attack to trick an admin user into running malicious queries.

[Exploit](#)[Third Party Advisory](#)[github.com](#)[text/html](#)

 MISC github.com/jra89/CVE-2019-20059

File Hosting Script - Online PHP File Hosting Script

[Product](#)[yetishare.com](#)[text/html](#)

 MISC yetishare.com/

YetiShare 3.5.2 — 4.5.4 Multiple vulnerabilities | by Jinny Ramsmark | Medium

[Exploit](#)[Third Party Advisory](#)[medium.com](#)[text/html](#)

 MISC medium.com/@jra8908/yetishare-3-5-2-4-5-4-multiple-vulnerabilities-927d17b71ad

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

Exploit/POC from Github

Yetishare SQL Injection in sSortDir_0 parameter - v3.5.2 - v4.5.4. Apart from an admin being able to exploit this, it...

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 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)