



CVE-2019-12099

Published on: 05/14/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12099

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

Certain versions of [Php-fusion](#) from [Php-fusion](#) contain the following vulnerability:

In PHP-Fusion 9.03.00, edit_profile.php allows remote authenticated users to execute arbitrary code because includes/dynamics/includes/form_fileinput.php and includes/classes/PHPFusion/Installer/Lib/Core.settings.inc mishandle executable files during avatar upload.

CVE-2019-12099 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	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
PHP-Fusion 9.03.00 - 'Edit Profile' Remote Code Execution (Metasploit)	Exploit Third Party Advisory VDB Entry	www.exploit-db.com/exploits/46839

[www.exploit-db.com](#)[Proof of Concept](#)[text/html](#)

Update form_fileinput and default mimecheck test · php-fusion/PHP-Fusion@9434320 · GitHub

[Patch](#)[Third Party Advisory](#)[web.archive.org](#)[text/html](#)[Inactive Link](#)[Not Archived](#)

MISC [github.com/php-fusion/PHP-Fusion/commit/943432028b9e674433bb3f2a128b2477134110e6](#)

Pentest Blog - Self-Improvement to Ethical Hacking

[Exploit](#)[Third Party Advisory](#)[www.pentest.com.tr](#)[text/x-ruby](#)

MISC [www.pentest.com.tr/exploits/PHP-Fusion-9-03-00-Edit-Profile-Remote-Code-Execution.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	Php-fusion	Php-fusion	All	All	All	All
Application	Php-fusion	Php-fusion	All	All	All	All

cpe:2.3:a:php-fusion:php-fusion:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →