



CVE-2020-27386

Published on: 11/12/2020 12:00:00 AM UTC

Last Modified on: 12/06/2022 09:18:00 PM UTC

CVE-2020-27386

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Flexdotnetcms](#) from [Flexdotnetcms Project](#) contain the following vulnerability:

An unrestricted file upload issue in FlexDotnetCMS before v1.5.9 allows an authenticated remote attacker to upload and execute arbitrary files by using the FileManager to upload malicious code (e.g., ASP code) in the form of a safe file type (e.g., a TXT file), and then using the FileEditor (in v1.5.8 and prior) or the FileManager's rename function (in v1.5.7 and prior) to rename the file to an executable extension (e.g., ASP), and finally executing the file via an HTTP GET request to /<path_to_file>.

CVE-2020-27386 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: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
FlexDotnetCMS 1.5.8 Arbitrary ASP File	CVE-2020-27386	MISC: packetstormsecurity.com/files/160411/FlexDotnetCMS

FlexDotNetCMS 1.5.8 Arbitrary ASP File Upload ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/mies/160411/FlexDotNetCMS-1.5.8-Arbitrary-ASP-File-Upload.html
What's in a name: RCE Hunting in CMSs via Unrestricted File Upload	Exploit Third Party Advisory blog.vonahi.io text/html	 MISC blog.vonahi.io/whats-in-a-re-name/
Release FlexDotNetCMS v1.5.9 · MacdonaldRobinson/FlexDotnetCMS · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/MacdonaldRobinson/FlexDotnetCMS/releases/tag/v1.5.9
Add flexdotnetcms v1.5.8 exploit module and docs by kalba-security · Pull Request #14339 · rapid7/metasploit-framework · GitHub	Exploit Patch Third Party Advisory github.com text/html	 MISC github.com/rapid7/metasploit-framework/pull/14339

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	Flexdotnetcms Project	Flexdotnetcms	All	All	All	All
Application	Flexdotnetcms Project	Flexdotnetcms	All	All	All	All
cpe:2.3:a:flexdotnetcms_project:flexdotnetcms:*:*:*:*:*:						
cpe:2.3:a:flexdotnetcms_project:flexdotnetcms:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← 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](#)