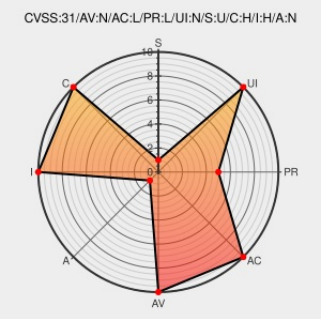
CVE-2020-27385

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

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-27385

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



Certain versions of Flexdotnetcms from Flexdotnetcms Project contain the following vulnerability:

Incorrect Access Control in the FileEditor (/Admin/Views/FileEditor/) in FlexDotnetCMS before v1.5.11 allows an authenticated remote attacker to read and write to existing files outside the web root. The files can be accessed via directory traversal, i.e., by entering a .. (dot dot) path such as ..\..\..\..\..\<file> in the input field of the FileEditor. In FlexDotnetCMS before v1.5.8, it is also possible to access files by specifying the full path (e.g., C:\<file>). The files can then be edited via the FileEditor.

CVE-2020-27385 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
What's in a name: RCE Hunting in CMSs via	Exploit	MISC blog.yonahi.io/whats-in-a-re-name/

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 v1.5.11 · MacdonaldRobinson/FlexDotnetCMS · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/MacdonaldRobinson/FlexDotnetCMS/releases/tag/v1.5.11

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

← Previous ID

Next ID→