binderlabs / DirCreate2System Public

sailay1996 Update README.md 2a48d7d · 2 years ago 5 Commits

bin	Add files via upload	2 years ago
src	Add files via upload	2 years ago
POC1.jpg	Add files via upload	2 years ago
README.md	Update README.md	2 years ago
poc.wmv	Add files via upload	2 years ago

README

DirCreate2System

Weaponizing to get NT AUTHORITY\SYSTEM for Privileged Directory Creation Bugs with Windows Error Reporting

Short Description:

I've discovered **comctl32.dll** (which is missing in system dir which doesn't really exist) has been loaded by wermgr.exe via windows error reporting by running schtasks. It means if we can create a folder name as **C:\windows\system32\wermgr.exe.local** with Full permission 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.

About

Weaponizing to get NT SYSTEM for Privileged Directory Creation Bugs with Windows Error Reporting

windows-exploitation

windows-privilege-escalation

Releases

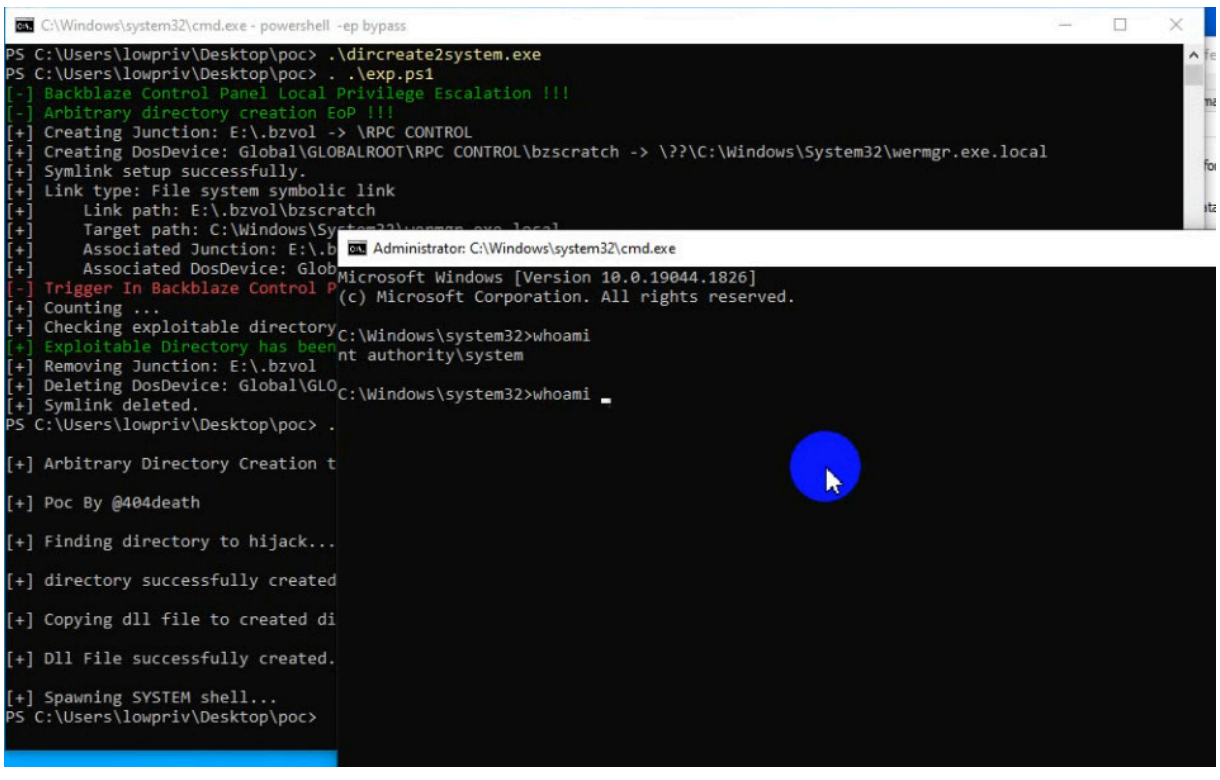
No releases published

Packages

No packages published

Languages

C++ 90.7% C 9.3%



Note: