

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://github.com/klinix5/InstallerFileTakeOver


Go


JANAPR21JUN202120222023


54 captures


22 Nov 2021 - 14 J


About this capture

 klinix5 / **InstallerFileTakeOver** Public

 Notifications

 Fork 422

 Star 1.7k



<> Code

Issues 1

Pull requests

Actions

Projects

Wiki

Security

Insights








 main ▾

 1 branch

 0 tags

Go to file

Code ▾

	klinix5 Update README.md	57f390e on 20 Dec 2021	 22 commits
	InstallerFileTakeOver	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

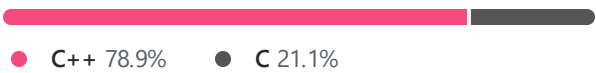
Packages

No packages published

Contributors 2

-  klinix5 Abdelhamid Naceri
-  0dayCTF Ryan Montgomery

Languages



README.md

InstallerFileTakeOver



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 successfully 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

[54 captures](#)
22 Nov 2021 - 14 J

JAN2021

APR212022

JUN2023

?

x

f

t

About this capture