Open in app ↗ Sign up Sign in

Medium Search Write

The trouble with Microsoft's Troubleshooters

Imre Rad · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

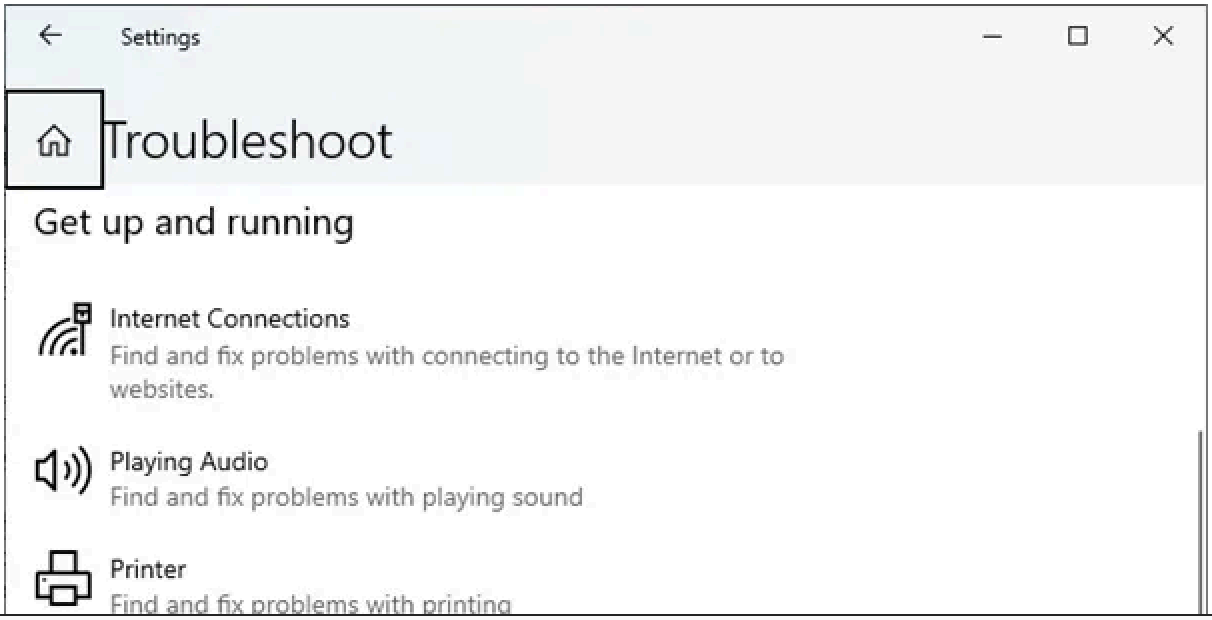
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month



Troubleshoot

Get up and running

Internet Connections
Find and fix problems with connecting to the Internet or to websites.

Playing Audio
Find and fix problems with playing sound

Printer
Find and fix problems with printing

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

So where is the problem then? A flaw in the implementation allows attackers to save any files to any locations on the file system (in line with the permissions of the current user) and this takes place before the integrity of the package is checked. Even though overwriting of files is not possible via this vulnerability due to another security measure, an attacker could still gain code execution here by dropping a file to the Startup folder of **Windows**, which will be executed by the Operating System next time when the user logs in.

Threat actors usually distribute malicious files like this in email, via their

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

servers blocking my attachments, however, by linking to a webdav share, I could circumvent this protection so the diagcab file could be executed in **Outlook.** But not even links like this can be used ultimately, they are deactivated by providers like **Gmail** or **Outlook Live** and blocked by other security measures of Internet Explorer.

Other popular products like **Google Chrome**, **Mozilla Firefox** or **Thunderbird** simply pop up the standard open and execute dialog box when they see *.diagcab* files. Actually, even **Microsoft Edge**. Using one of these browsers for reading emails on a web based platform is probably the biggest

Medium

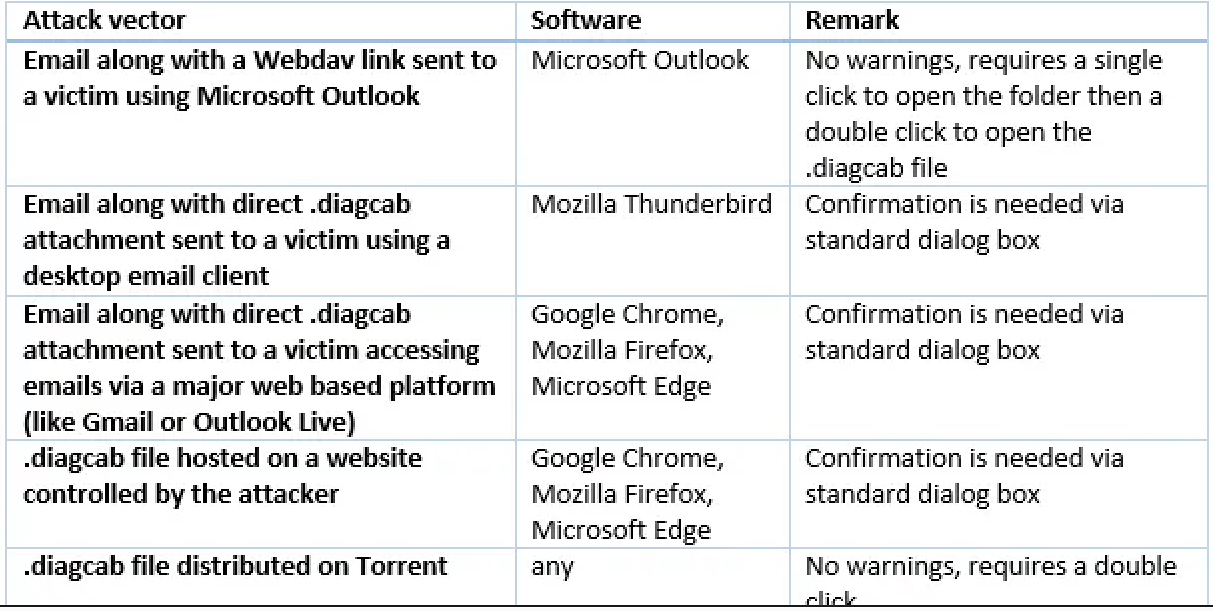
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Attack vector	Software	Remark
Email along with a Webdav link sent to a victim using Microsoft Outlook	Microsoft Outlook	No warnings, requires a single click to open the folder then a double click to open the .diagcab file
Email along with direct .diagcab attachment sent to a victim using a desktop email client	Mozilla Thunderbird	Confirmation is needed via standard dialog box
Email along with direct .diagcab attachment sent to a victim accessing emails via a major web based platform (like Gmail or Outlook Live)	Google Chrome, Mozilla Firefox, Microsoft Edge	Confirmation is needed via standard dialog box
.diagcab file hosted on a website controlled by the attacker	Google Chrome, Mozilla Firefox, Microsoft Edge	Confirmation is needed via standard dialog box
.diagcab file distributed on Torrent	any	No warnings, requires a double click

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

✦ Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

```
<?xml version="1.0" encoding="utf-8"?>

<PackageConfiguration
xmlns="http://www.microsoft.com/schemas/dcm/configuration/2008">

<Execution>

<Package Path="%windir%\diagnostics\system\Audio">

<Answers Version="1.0">

<Interaction ID="IT_GetDeviceType">

<Value>microphone/headset microphone</Value>

</Interaction>

</Answers>
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

The Path attribute of the referenced packages point to a directory in the file system. Packages under *%WINDIR%\Diagnostics* folder are considered to be valid without any further checking, but anything else is subject to signature verification. This is implemented in the helper library *sdiageng.dll*. Before verifying the signature, the implementation makes a local copy of the referenced directory to a temporary random destination folder, something like "*C:\Users\John Doe\AppData\Local\Temp\SDIAG_0636db01-fabd-49ed-bd1d-b3fbbe5fd0ca*". Note this path has a static number of components which will make the attack deterministic.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
while (FindNextFile(hFind, &FindFileData) != 0);FindClose(hFind);
```

After the copy is done, the *dll* verifies the integrity based on the file *DiagPackage.cat*. If everything is correct and the user proceeds with the wizard on the GUI, the embedded powershell scripts are executed under the hood.

Here comes the trick: since the data source is controlled by the attacker and

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
2017. 07. 12.  11:10    <DIR>          ..

2017. 07. 12.  10:48            27 648
..\..\..\..\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\calc.exe

1 File(s)         27 648 bytes

2 Dir(s)  251 292 504 064 bytes free
```

Putting this altogether, the crafted *.diagcab* file has the package path set to the rogue webdav server. Once it is opened by the victim, a new file is saved under the *Startup* directory, and is executed by the operating system on the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Demo

Diagcab files and a rogue webdab PoC server is hosted online for demonstrational purposes. (This latter will go down once my free dyno hours are exhausted at Heroku.)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
dir \\webdav-test.herokuapp.com@SSL\DavWWWRoot
```

If you execute the diagcab file hosted here, it will configure your Windows to launch the calculator at login. To revert the original status of your computer press CTRL+R, type shell:startup and remove the calc.exe file from the folder.

Sources of the webdav server exploit can be found on Github:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

8/4/2022: Microsoft have reassessed the case "This email may come as a bit of a surprise, but this is a follow up to your case MSRC 55532 which was submitted back in 2019. We have reassessed the issue per our updated Windows bug bar (https://aka.ms/windowsbugbar) and determined that this issue meets our criteria for servicing with a security update." (CVE-2022–34713)

Microsoft's response

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

> *bypassed, the PoC doesn't escalate permissions in any way, or do anything the user couldn't do already.*

Poll

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Written by Imre Rad

Follow

104 Followers

Software developer daytime, security researcher in freetime

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app