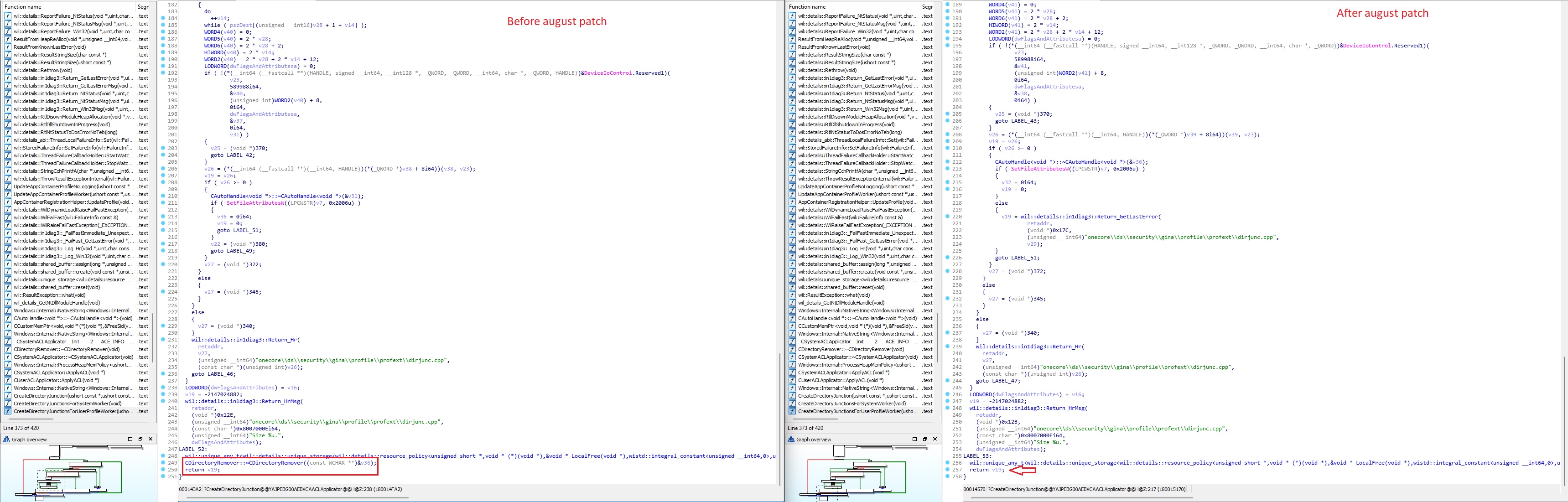
**Description:**

Technically, in the previous report [CVE-2021-34484](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34484). I described a bug where you can abuse the user profile service to create a second junction.  
But as I see from ZDI advisory and Microsoft patch, the bug was metered as an arbitrary directory deletion bug.  
Microsoft didn’t patch what was provided in the report but the impact of the PoC. Since the PoC I wrote before was horrible, it could only reproduce a directory deletion bug.

As from the Quick patch analysis, they didn’t do any major changes to the code

  
profext.dll!CreateDirectoryJunction

They only removed the CDirectoryRemover destructor which remove the directory. Unfortunately, this isn’t sufficient to fix the bug.

Why?

Simply because the lock mechanism still fails to lock the directory correctly. Hence, we can abuse the service to create a second directory junction in arbitrary locationHe



The code snippet above show how the locking mechanism work.  
First of all the service create the target directory and call PathCchRemoveFileSpec to get a string of the parent directory, next it will call CreateFileW with GENERIC\_READ and FILE\_SHARE\_READ in the desired access and the allowed sharing. In the end, the service ensure that the parent directory isn’t a junction by calling GetFileInformationByHandleEx.

This normally should be able to fix any junction related bug, but it doesn’t.  
This code only expect that we cannot control both directories parent, in our case we can.

In CVE-2021-26426, I have chosen “C:\Users\Temp\Documents\My Pictures” junction creation as a target. Microsoft patch is right in this case, we can clearly see that C:\Users\Temp isn’t controllable by the user due to the locking introduced by the user profile service.  
But not in case of "C:\Users\Temp\AppData\Local\History", here we control their parent folder C:\Users\Temp\AppData because it’s not locked by the service. We can clearly make the AppData folder a junction to somewhere else, so both CreateFileW and GetFileInformationByHandleEx checks will succeed.

And done, we will have our arbitrary junction creation bug again!

The PoC has been tested on windows 11 with October 2021 patch.