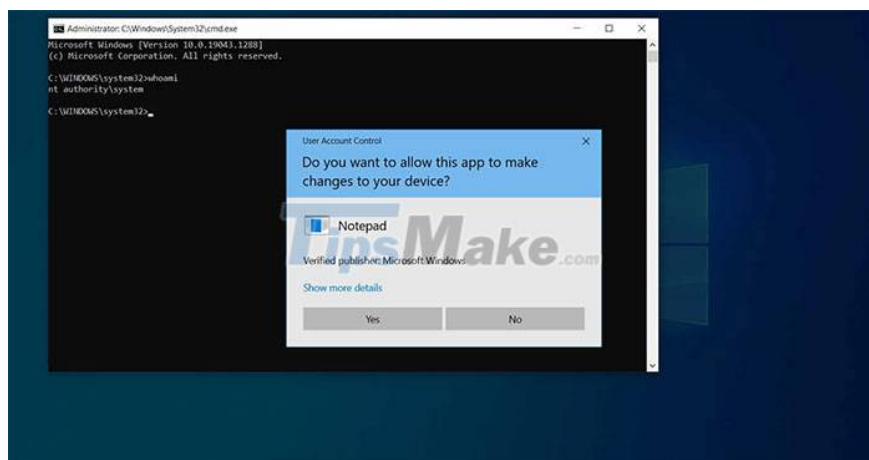


# There is a Windows error that Microsoft can't fix forever, so a third party has to fix it

The Windows bug with code CVE-2021-34484 has been patched by Microsoft before, but it is still not really complete, so Opatch has to be patched again.

**CVE-2021-34484** is a Windows local privilege escalation zero-day vulnerability that allows users with administrative rights in Windows 10, Windows 11, and Windows Server.

This vulnerability scores 7.8 in the CVSS v3. So far, there is no sign of this vulnerability being exploited by attackers, but there are still many potential risks.



In August 2021, Microsoft released an official patch for this vulnerability shortly after it was discovered. After that, this bug was marked as fixed, but in fact, Microsoft's patch only fixed part of the problem, the vulnerability still existed.

A few months ago, Opatch discovered this vulnerability in the Windows User Profile Service. So Opatch took action and self-released the patch profext.dll.

By January 2022, Microsoft fixed this bug and replaced the "profext.dll" file, which caused the unofficial fix to be removed from everyone who applied the January Windows updates. 2022. In fact, Microsoft's patches did not fix the error, even breaking the previous unofficial patch of Opatch.

Opatch continues to have to update its patch to be compatible with the latest Microsoft Tuesday Update and provide it for free to all registered users.

Affected and updated versions of Windows include:

1. Windows 10 v21H1 (32 & 64 bit) updated with the March 2022 Update
2. Windows 10 v20H2 (32 & 64 bit) updated with March 2022 Update
3. Windows 10 v1909 (32 & 64 bit) updated with the March 2022 Update
4. Windows Server 2019 64 bit updated with March 2022 Update

Microsoft said that it is aware of this case and will take appropriate steps to protect the safety of users.

You finished reading the article "**There is a Windows error that Microsoft can't fix forever, so a third party has to fix it**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.