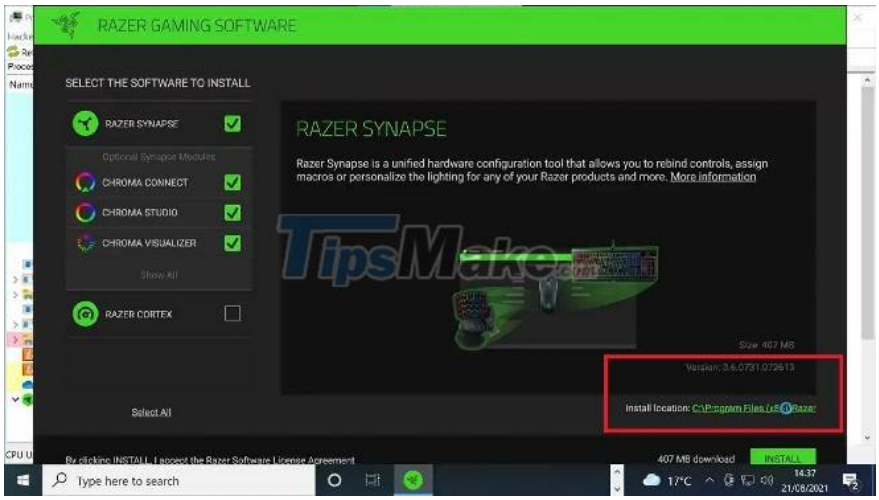
You can gain admin rights of Windows 10 just by plugging in a Razer mouse

The PrintNightmare vulnerability makes the hacker community and security researchers pay attention to vulnerabilities that appear on Microsoft products when installing third-party drivers.

Recently, researcher Jonhat discovered a new vulnerability that allows to gain admin rights of Windows 10 just by plugging a Razer mouse into the computer.

Specifically, when plugging in a Razer mouse or the USB end of a Razer wireless mouse, Windows Update will download and execute the RazerInstaller driver under admin rights. Next, Razer's driver installer and device customization software allows users to open an Explorer window to choose where to store the installation files.



On that Explorer window, just press Shift + Right-click and a Powershell window with admin rights will be displayed. Basically, a skilled hacker can use a Powershell window with admin rights to do whatever he wants.

In addition, if the user performs the installation and specifies the directory to save the installation file in a user-controllable path such as the Desktop, the installer will save a service binary there. This binary can be edited to execute code before the user logs in on startup.

Hackers don't even need a real Razer mouse because the USB ID can be spoofed easily.

Jonhat said he tried to contact Razer but was unsuccessful. So he decided to make it public. It is likely that Microsoft will soon recognize the problem and proceed to remove the Razer driver from Windows Update. However, Razer's involvement is still required to edit their drivers before hackers can exploit this vulnerability.

tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.