Hundreds of millions of Windows 10 computers are easily hacked due to errors in the original software of the manufacturer

Many Windows 10 computers exist because of manufacturer flaws that put them at risk of being attacked by hackers.

The continuous failure of Windows 10 updates has made Microsoft face many difficulties in the past. But Microsoft's partners have contributed to the deterioration of the company's situation.

Recently, the well-known security company SafeBreach Labs in California has disclosed information, many Windows 10 computers exist vulnerabilities of manufacturers that put them at risk of attack by hackers. This vulnerability lies in PC-Doctor Toolbox analysis software installed on many devices of Dell, Alienware, Staples and Corsair .

Pre-installed software puts Dell computers at high risk of malicious code infection. Photo: Dell.

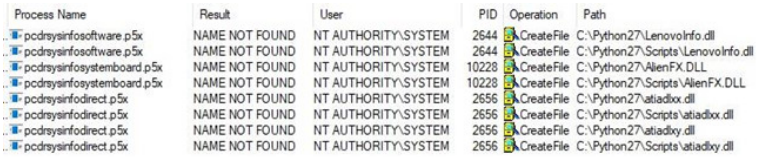
Dell, the world's largest computer maker, said PC-Doctor Toolbox is customized as SupportAssist available on most of its products. Last year, the computer maker shipped nearly 60 million computers.

On March 29th, SafeBreach discovered on Dell computers that there was a serious error that allowed hackers to change the DLL to spread malicious code to control the computer system. Last month, Dell confirmed and released a patch for the bug.

SupportAssist is a software for diagnosing the health of the system's health, so it has access to physical memory, PCI, SMBios . When the tool is infected with malicious code, the hacker can control the user's computer.

The affected module on SupportAssist is a version of PC-Doctor Toolbox and was found on many other manufacturers' devices. Immediately after discovering the incident, the parties have actively sought solutions to solve this problem but so far have not been able to solve it thoroughly.

Many similar cases have been discovered by SafeBreach. Windows 10 users who believe in using the original software of the manufacturer do not know they are in danger.



Process Name	Result	User	PID	Operation	Path
pcdrsysinfosoftware.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2644	CreateFile	C:\Python27\LenovoInfo.dll
pcdrsysinfosoftware.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2644	CreateFile	C:\Python27\Scripts\LenovoInfo.dll
pcdrsysinfosystemboard.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	10228	CreateFile	C:\Python27\AlienFX.DLL
pcdrsysinfosystemboard.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	10228	CreateFile	C:\Python27\Scripts\AlienFX.DLL
pcdrsysinfodirect.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2656	CreateFile	C:\Python27\atiadlxx.dll
pcdrsysinfodirect.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2656	CreateFile	C:\Python27\Scripts\atiadlxx.dll
pcdrsysinfodirect.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2656	CreateFile	C:\Python27\atiadlxy.dll
pcdrsysinfodirect.p5x	NAME NOT FOUND	NT AUTHORITY\SYSTEM	2656	CreateFile	C:\Python27\Scripts\atiadlxy.dll

DLL files are vulnerable to malicious code. Photo: Safebreach.

Windows already has many bugs that make users uncomfortable, but because Microsoft cannot interfere with the manufacturer's original software installation process, the problem is even more serious. This makes Windows less secure.

As recommended by Forbes, customers should check the default programs, can remove unnecessary software when buying a new computer.

You finished reading the article "**Hundreds of millions of Windows 10 computers are easily hacked due to errors in the original software of the manufacturer**" 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.

© 2019 TipsMake.com