There is a new zero-day vulnerability in Windows

The vulnerability posted on Twitter and on GitHub also has a PoC that demonstrates one of the ways this error exploits the machine, making it impossible to boot.

The vulnerability posted on Twitter and on GitHub also has a PoC that demonstrates one of the ways this error exploits the machine, making it impossible to boot.

SandboxEscaper, an August researcher who posted a Windows escalation error, recently discovered an unpatched Windows vulnerability on his Twitter.

The new error also has some similarities to the previous error.Windows services are often run with privileges and sometimes they perform some action on behalf of the user with a feature called impersonation.These services act as if they are using a user's privilege.Then they return to their original identities.

Both this error and the previous error that SandboxEscaper detected are based on using an improper impersonation feature, specifically the service (last time Task Scheduler, Data Sharing Service this time) to transfer the identity quickly and effectively. currently acts with advanced rights.

The latest error allows a file to overwrite another file, causing the impersonated file to be deleted, making it impossible for users who have no permissions to delete any files on the system, even those data they should not have access to.

New vulnerabilities only affect Windows 10, Server 2016 and Server 2019

The point of time with this error is very important, two actions must be done simultaneously to be successful.SandboxEscaper says that, therefore, deploying on a single-core machine may seem difficult, but with

multiple-core machines it is very vulnerable to attack.The PoC of SandboxEscaper posted on GitHub will prove by deleting the Windows PCI driver.Users should not try it at an important machine because when this file is deleted, the machine cannot boot.

Data Sharing Service is only available on Windows 10, so this error will only affect Windows 10, Windows Server 2016 and Windows Server 2019. The error was previously used on malware.New errors are harder to exploit and the ability to delete files is also not useful by overwriting the file.

See more:

1. The new zero-day vulnerability on Windows 10 helps hackers take control of the computer
2. Security vulnerabilities - basic insights
3. Good hackers find and patch the vulnerability for more than 100,000 other routers