Discover new Zero-Day vulnerabilities that target bugs in Windows 10 Task Scheduler

SandboxEscaper, a vulnerability researcher named SandboxEscaper, recently quietly announced the emergence of a new zero-exploit in Windows 10 operating system less than a week after the operating system received it. Get regular updates from Microsoft.

SandboxEscaper, a vulnerability researcher nicknamed SandboxEscaper, recently quietly announced the emergence of a new zero-exploit feature in the Windows 10 operating system platform, which is less than a week after the operating system This operator receives periodic updates from Microsoft.

This was the fifth exploit in a series of complex exploits aimed at Windows 10, which began to appear at the end of August last year. This time, it has achieved local privilege escalation, giving the author full control over file systems that are only for users with full privileges like SYSTEM and TrustedInstaller.

1. Microsoft rushed to release security updates for Windows XP, Server 2003

'Malformed' tasks

Once again, SandboxEscaper focused on Task Scheduler utility and used it to import old tasks from other systems. Basically, Task Scheduler is a utility that owns many useful features for the system, including the ability to automate the necessary tasks or the programs that users want on Windows. At the time of Windows

XP, tasks were usually in the .JOB format and they could still be added to newer versions of the operating system.

When this process takes place, Task Scheduler will proceed to import the job file with any DACL control (arbitrary access control list). When no DACL is available, the system will be able to grant any user full access to the file.

1. Mysterious hackers offer Windows zero-day vulnerabilities to the world's most dangerous cyber criminals

The researcher explained that this error can be exploited by importing old task files into the Task Scheduler utility on Windows 10. Running a command using 'scht task.exe' and 'calendarsvc.dll' is possible. Copy from the old system, this will lead to a remote procedure call (RPC) to "_SchRpcRegisterTask" - a method of registering the task with the server, presented and processed by the translation Task Scheduler service.

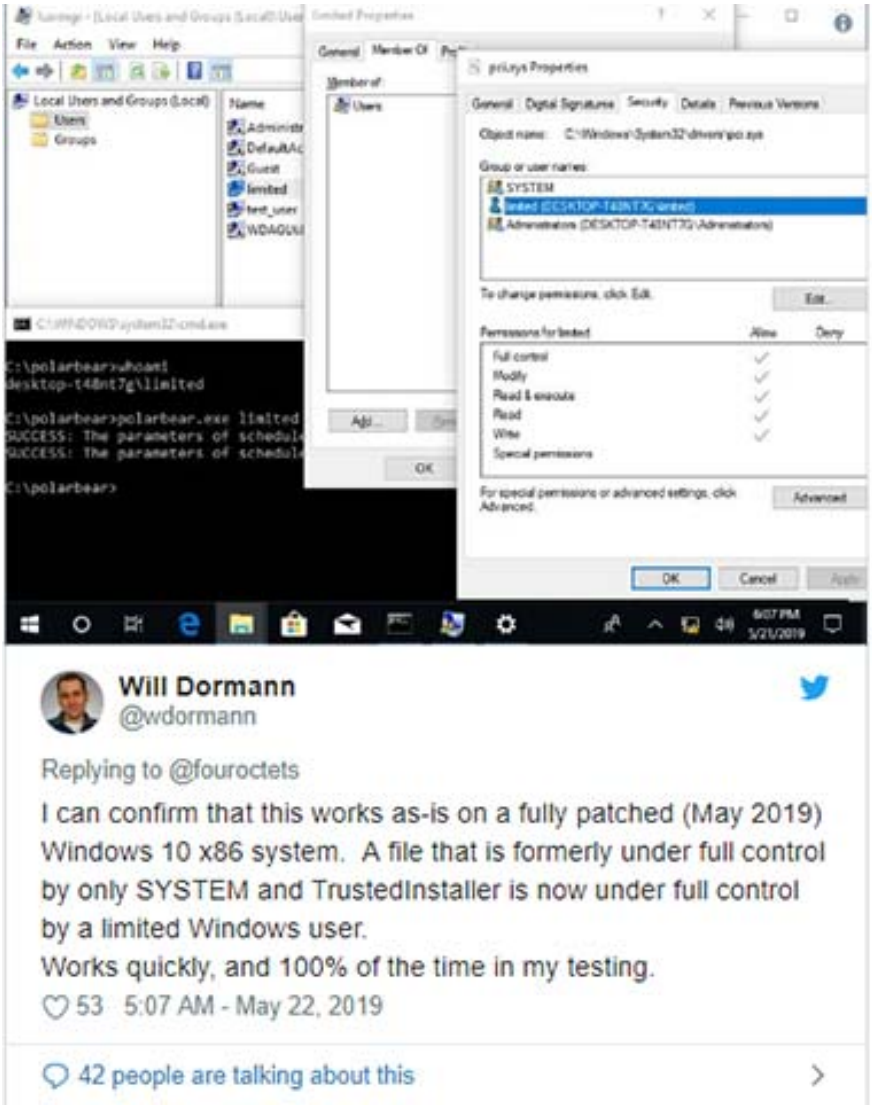
"I assume that to enable the above error, you just need to call directly into this function without having to use scht task.exe copied from windows xp ', SandboxEscaper said.

At the same time, this security researcher also believes that what begins with limited privileges ends with SYSTEM rights when encountering a specific function. To prove the validity of this task, SandboxEscaper shared a video showing that the PoC is operating on Windows x86.

1. Detects Zero-Day vulnerabilities on Windows PC operating systems that allow administrative rights

SandboxEscaper also released the exploit on GitHub, and this is said to be a warning to Microsoft. The exploits of this security researcher were previously used in malware, and at the same time the female hacker also said she found 3 more exploits of local privilege escalation on Windows 10, intended to will be released in the near future.

This exploit of SandboxEscaper is now confirmed by Will Dormann, a reputable security vulnerability analyst at the CERT dispatch center.



1. Counter-Strike 1.6 features new Zero-Day, allowing malicious servers to hack gamers' computers

With this vulnerability, Microsoft is likely to release patches right away in Patch Tuesday next month or at the latest in July.