Windows Task Scheduler Zero Day Exploited by Malware

bleepingcomputer.com/news/security/windows-task-scheduler-zero-day-exploited-by-malware/

Ionut Ilascu

By

Ionut Ilascu

- September 5, 2018
- 11:45 AM
- 4

Malware developers have started to use the zero-day exploit for Task Scheduler component in Windows, two days after proof-of-concept code for the vulnerability appeared online.

A security researcher who uses the online name SandboxEscaper on August 27 released the source code for exploiting a security bug in the Advanced Local Procedure Call (ALPC) interface used by Windows Task Scheduler.

More specifically, the problem is with the SchRpcSetSecurity API function, which fails to properly check user's permissions, allowing write privileges on files in C:\Windows\Task.

The vulnerability affects Windows versions 7 through 10 and can be used by an attacker to escalate their privileges to all-access SYSTEM account level.

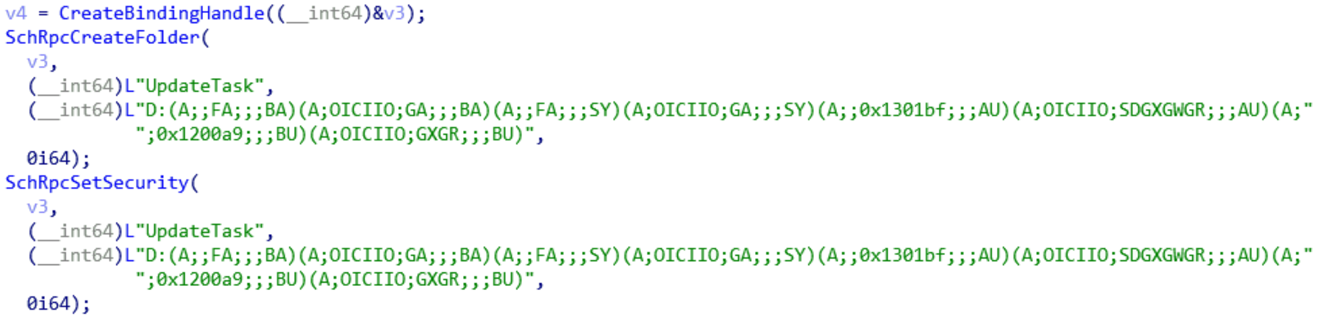
A couple of days after the exploit code became available (source and binary), malware researchers at ESET noticed its use in active malicious campaigns from a threat actor they call PowerPool, because of their tendency to use tools mostly written in PowerShell for lateral movement.

PowerPool targets GoogleUpdate.exe

The group appears to have a small number of victims in the following countries: Chile, Germany, India, the Philippines, Poland, Russia, the United Kingdom, the United States, and Ukraine.

The researchers say that PowerPool developers did not use the binary version of the exploit, deciding instead to make some subtle changes to the source code before recompiling it.

"PowerPool's developers chose to change the content of the file C:\Program Files (x86)\Google\Update\GoogleUpdate.exe. This is the legitimate updater for Google applications and is regularly run under administrative privileges by a Microsoft Windows task," ESET notes.



```
v4 = CreateBindingHandle((__int64)&v3);
SchRpcCreateFolder(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
            ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
SchRpcSetSecurity(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
            ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
```

Threat actor changes permissions of the Google Updater executable

This allows PowerPool to overwrite the Google updater executable with a copy of a backdoor they typically use in the second stages of their attacks. The next time the updater is called, the backdoor launches with SYSTEM privileges.

According to the researchers, PowerPool malware operators likely use the second-stage backdoor only on victims of interest, following a reconnaissance step.

Microsoft did not patch the ALPC bug to this day, but it is expected to release a fix in its monthly security updates, on September 11.

Some mitigation is possible without Microsoft's help, though the company did not approve it. A solution provided by Karsten Nilsen blocks the exploit and allows scheduled tasks to run, but it may break things created by the legacy Task Scheduler interface.

> Short term solution on VU#906424:
> icacls c:\windows\tasks /remove:g "Authenticated Users"
> icacls c:\windows\tasks /deny system:(OI)(CI)(WD,WDAC)
> Tested and blocks 0day, changing these rights may result in unexpected behavior in scheduled tasks.@USCERT_gov
>
> — Karsten Nilsen (@karsten_nilsen) August 28, 2018

Users of 64-bit Windows 10, version 1803, can mitigate the problem by applying a micropatch. The fix is temporary and requires the installation of the 0patch Agent from Acros Security.

The company makes the source code for the micropatch available in the tweet below:

> Blog post is in the making but for the impatient, here's the source code of our micropatch. Three patchlets, one calling RpcImpersonateClient, one removing a premature call to RpcRevertToSelf, and one adding a RpcRevertToSelf call where it should be. Just 4 instructions. pic.twitter.com/PtgsPJiiSO
>
> — 0patch (@0patch) August 30, 2018

Related Articles:

Critical Windows RPC CVE-2022-26809 flaw raises concerns — Patch now

Exploit released for critical VMware auth bypass bug, patch now

Microsoft shares mitigation for Windows KrbRelayUp LPE attacks

Microsoft adds support for WSL2 distros on Windows Server 2022

Microsoft adds Office subscriptions to Windows 11 account settings

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.