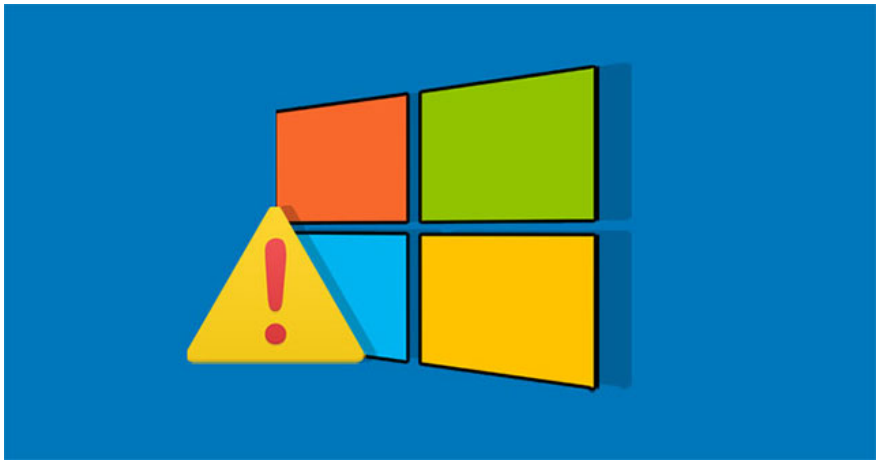
Google Project Zero reveals a serious privilege escalation vulnerability in Windows

Google Project Zero is one of the highly regarded professional security organizations today. The team's findings are not only important to the Google product itself, but also for other software products and services of other developers.

According to Google Project Zero, after a security vulnerability is discovered, the team 's experts will actively contact the software owner to provide detailed information about the vulnerability. The developer will have 90 days to fix the issue before Google makes the vulnerability public. Depending on the complexity of the fix request, Google will occasionally loosen the time it takes for a developer to patch.

On December 24, the Google Project Zero team publicly revealed a serious security bug in Windows. If successfully exploited, this vulnerability could lead to dangerous privilege escalation on victim systems.

The process leading to the vulnerability is quite complicated. However, it can be summarized as follows: A malicious process can send a Local Procedure Call (LPC) message to the Windows splwow64.exe process, through which an attacker can write any value to one. arbitrary addressing in the memory space of splwow64. Essentially, that means that an attacker can control this target address as well as any content copied to it.



In fact, this is not necessarily a new flaw. Prior to Google Project Zero, a security researcher at Kaspersky reported it earlier this year, and Microsoft also released a patch in June. However, this patch has been analyzed and confirmed by Google Project Zero. Determination is incomplete. The Microsoft security team says Microsoft's fix is ??not yet thorough, meaning that attackers can still exploit the vulnerability by making some tweaks in the exploit process.

This zero-day was individually reported to Microsoft by Google Project Zero on September 24, with a standard 90-day deadline for the Redmond company to fix the issue with a deadline of December 24.

Microsoft originally planned to release the fix in November, but the time frame was pushed back to December. After that, Microsoft continued to respond to Google that they had identified some additional issues. is currently in beta and will release a full patch by January 2021.

On December 8, the two sides met to discuss the patch release progress and next steps. As a result, Google Project Zero did not agree to extend Microsoft's time, and the vulnerability along with the proof-of-concept code was publicly revealed on the 24th as above.

Google's technical report does not state which version of Windows the vulnerability affects. However, Kaspersky's announcement from a few months ago suggests that attackers were using it to target new builds of Windows 10.

Not long ago, the Project Zero team also accidentally discovered a critical zero-day vulnerability that existed on the Windows platform, directly affecting versions from Windows 7 to Windows 10 version 1903 (coded identifier CVE-2020-17087), and a Chrome vulnerability with identifier CVE-2020-15999.