A new Windows 10 vulnerability allows attackers to gain full control of a computer.

A security researcher known as SandboxEscaper has just announced the appearance of a new zero-day vulnerability in Windows 10, allowing attackers to gain full control of a user's computer. The vulnerability was previously reported by ZDNet.

A new zero-day vulnerability in Windows 10 is also known as "local privilege escalation." When exploited, the vulnerability gives an attacker or malware control over the victim's computer by elevating their privileges to the System level.

This is quite a tricky problem because most malware can be limited by the user account restrictions it infects. Privilege escalation is broken, giving malware higher access.

A new vulnerability has been discovered in **Windows Task Scheduler** . An attacker can create a malicious **.job** file , then delete it and point to a kernel-level driver file from where the file was deleted, then recreate the task to stealthily allow a low-level process access to the system kernel.

This effectively grants the attacker system privileges across the entire device, allowing them to do anything they want on the victim's computer.

The tests worked on both 32-bit and 64-bit Windows. Additionally, according to Catalin Cimpanu of ZDNet, after some tweaking, he was able to successfully attack all versions of Windows from Windows XP and earlier, but failed on Windows 7 and Windows 8.

With the newly reported zero-day vulnerability, Microsoft will most likely release a patch on Patch Tuesday next month, expected on June 11th. However, until then, no one can be sure whether **the Windows 10 vulnerability** will be exploited in the wild.

Additional information : SandboxEscaper added two new local escalation vulnerabilities to GitHub early on May 22nd. One vulnerability, called " **angrypolarbearbug2** ," is a difficult-to-replicate strain that only affects specific hardware components. The other vulnerability, called " **sandboxescape,"** has an unclear purpose but involves infecting Internet Explorer 11 with malware to allow a remote attacker to escape the sandbox.