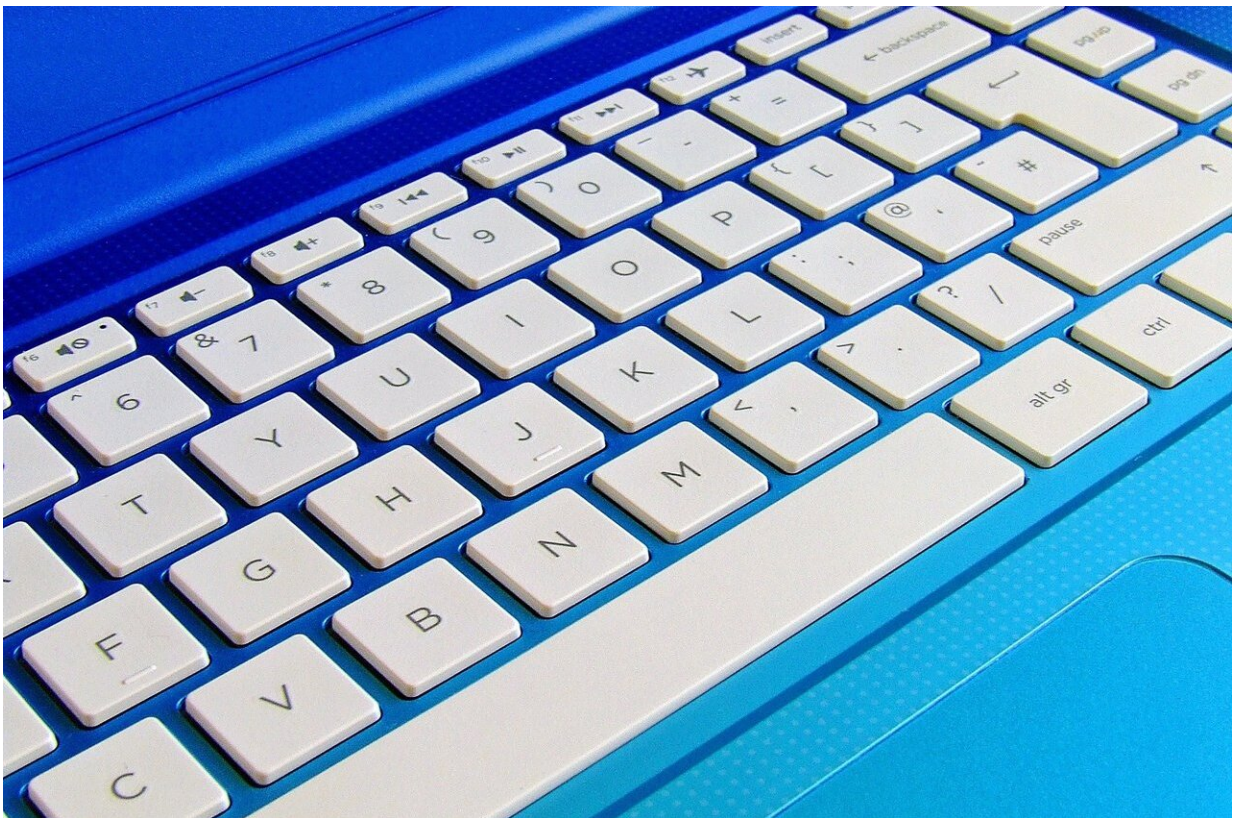


Microsoft patch awaited for zero-day vulnerability

August 31 2018, by Nancy Owano



Credit: CC0 Public Domain

A Windows zero-day bug has made the news. By zero-day, it means that a vulnerability has been exposed but it is not yet patched.

Darren Allan in *TechRadar* was one of the tech watchers reporting on the [vulnerability](#), which could occur through a privilege escalation bug.

Who found the hole? Allan said it was Twitter user SandboxEscaper.

So, just an attention-seeking gimmick wasting time in false claims with no grounds for concern?

No.

"The user linked to a page on GitHub which appears to contain a proof-of-concept (PoC) for the vulnerability," said Charlie Osborne in *ZDNet*.

"CERT/CC (the US cybersecurity organization which looks to counter emerging threats) has confirmed that this vulnerability can be leveraged against a 64-bit Windows 10 PC which has been fully patched up to date, " said *TechRadar*, in turn referring to a story in *The Register*,

Richard Chergwin, *The Register*, had reported that "CERT/CC vulnerability analyst Will Dormann quickly verified the bug."

CERT/CC did a formal [investigation](#), and posted an advisory.

"'Microsoft Windows task scheduler contains a vulnerability in the handling of ALPC, which can allow a local user to gain SYSTEM privileges,' the alert stated."

Last revised: 30 Aug 2018, the Vulnerability Note VU#[906424](#) said, "The Microsoft Windows task scheduler SchRpcSetSecurity API contains a vulnerability in the handling of ALPC, which can allow an authenticated user to overwrite the contents of a file that should be protected by filesystem ACLs. This can be leveraged to gain SYSTEM privileges. We have confirmed that the public exploit code works on 64-bit Windows 10 and Windows Server 2016 systems. We have also

confirmed compatibility with 32-bit Windows 10 with minor modifications to the public exploit code. Compatibility with other Windows versions is possible with further modifications."

Should we worry? Allan said it is a local bug. The attacker would have to be already logged into the [PC](#) to exploit it, or be running code on the machine.

But wait. Though local, *Ars Technica's* Peter Bright let its readers know what the flaw allows one to do. Not pretty.

Bright wrote that "The flaw allows anyone with the ability to run code on a system to elevate their privileges to 'SYSTEM' level, the level used by most parts of the operating system and the nearest thing that Windows has to an all-powerful [superuser](#)."

[Osborne](#) in *ZDNet* said that while the impact was limited, "the public disclosure of a zero-day is still likely a headache for the Redmond giant."

A zero-day bug is a reasonable explanation of why Sandbox was in the news but it was the way in which the bug was revealed that made news too:

Chapter One: it was publicly outed.

TechRadar: "...it seems that someone got frustrated with Microsoft's procedures for submitting bugs and vulnerabilities, and decided just to go ahead and publicly out the vulnerability instead."

Chapter Two: Microsoft is a cool company.

SandboxEscaper, though, subsequently tweeted: "I screwed up, not

MSFT (they are actually a cool company). Depression sucks."

A patch is doubtless in the works, said *TechRadar*. "It is not clear as to when the [patch](#) will arrive," said *Silicon Republic*, "but Microsoft's next scheduled Patch Tuesday is 11 September."

"Windows has a customer commitment to investigate reported security issues, and proactively update impacted devices as soon as possible," a Microsoft spokesperson stated. "Our standard policy is to provide solutions via our current Update Tuesday [schedule](#)."

© 2018 Tech Xplore

Citation: Microsoft patch awaited for zero-day vulnerability (2018, August 31) retrieved 2 March 2024 from <https://techxplore.com/news/2018-08-microsoft-patch-awaited-zero-day-vulnerability.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.