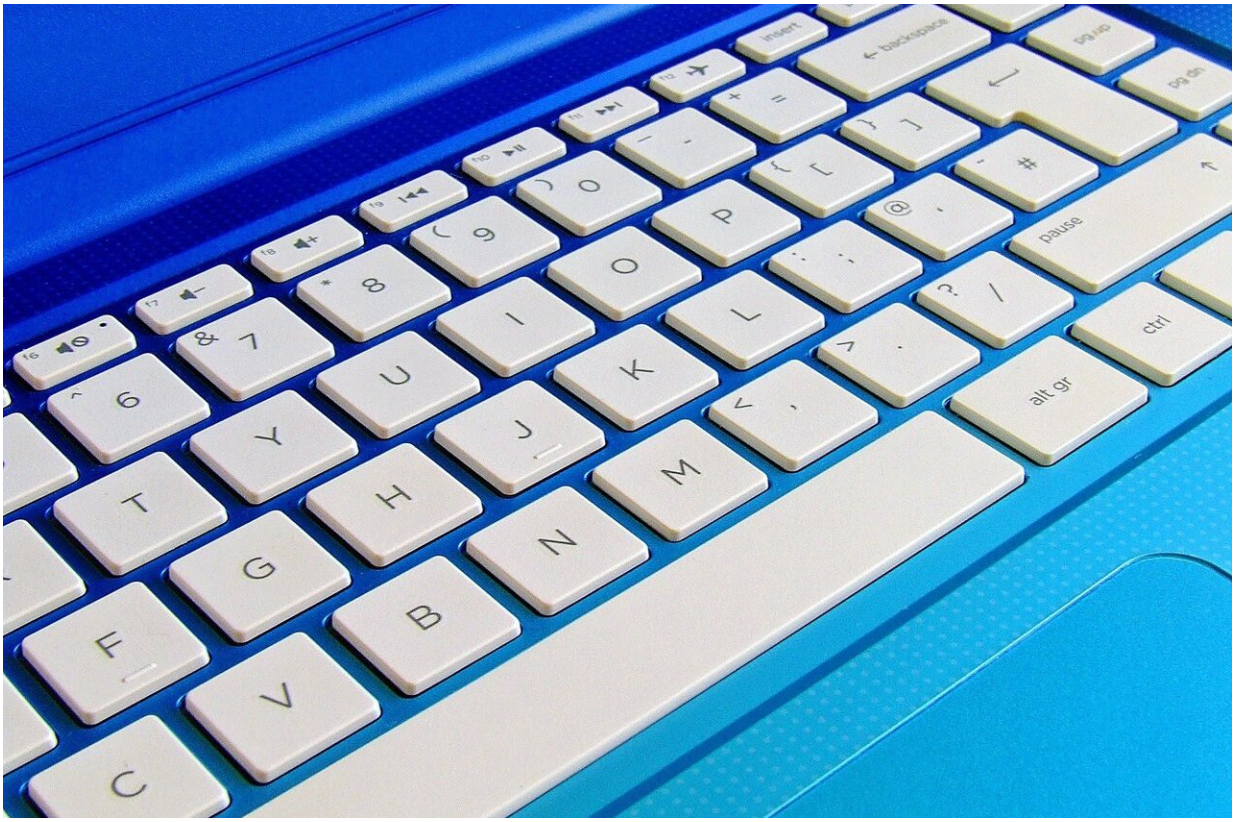
Zero-day bug found in Windows 10, disclosed on Twitter

October 25 2018, by Nancy Owano



Credit: CC0 Public Domain

Another day, another zero-day scare for Windows 10. The latest flaw was published on Twitter, said reports.

Darren Allan in *TechRadar* was one of a number of writers to cut to the quick. The vulnerability involved the Microsoft Data Sharing Service (dssvc.dll), which facilitates data brokering between running applications.

To be precise, the flaw was "an elevation-of-privilege zero-day vulnerability in Microsoft's Data Sharing Service (dssvc.dll) " wrote Tara Seals in *Threatpost*.

Which systems are affected? The vulnerability affects flavors of Windows 10 that include the latest October 2018 Update, for those who have installed it – along with Windows Server 2016 and 2019, said *TechRadar*.

Catalin Cimpanu in *ZDNet* similarly said that, according to several security experts, the zero-day only affects recent versions of the Windows OS, such as Windows 10 (all versions, including the latest October 2018 Update), Server 2016, and even the new Server 2019.

> https://t.co/1Of8EsOW8z Here's a low quality bug that is a pain to exploit.. still unpatched. I'm done with all this anyway. Probably going to get into problems because of being broke now.. but whatever.
>
> — SandboxEscaper (@SandboxEscaper) October 23, 2018

Earlier Windows versions that did not carry Data Sharing Service are not affected. That means it does not affect Windows 8.1 or earlier incarnations of Microsoft's desktop OS, Allan wrote.

Will Dormann relayed the message about systems not affected. "Confirmed as well on Win10 1803, fully-patched as of October. It's perhaps worth noting that the service used by the PoC, Data Sharing

Service (dssvc.dll), does not seem to be present on Windows 8.1 and earlier systems."

The discoverer tweeted about the bug and released a proof of concept. The person who made the discovery? Shaun Nichols reported on the "skilled Microsoft bug hunter" who goes by the name of SandboxEscaper.

What damage, in theory, could an exploit cause? *Threatpost* referred to it in its headline as a "Windows 'Deletebug' Zero-Day," for a reason.

"The code exploits a vulnerability that allows deleting without permission any files on a machine, including system data," said Ionut IlascuI in *BleepingComputer*, "and it has the potential to lead to privilege escalation."

Easy or difficult to wreak havoc? Well, it was described as a low-quality bug that is a pain to exploit. Shaun Nichols in *The Register* repeated that "the flaw will be difficult for an attacker to successfully exploit in the wild." He also pointed out what that might mean for those waiting for a Microsoft response. "That also likely means that Microsoft will opt not to issue an out-of-band update for the coding cockup, and wait until next month's Patch Tuesday to post a permanent fix for the vulnerability."

Nichols warned readers, "Don't touch it unless you know what you're doing." He issued the warning relating to the researcher having provided a proof-of-concept on GitHub and tweeted out a link. Nichols wrote, "WARNING: it will crash your Windows 10 PC into recovery mode, and require you to revert your filesystem back to a previous good backup. Don't touch it unless you know what you're doing."

Jonny Caldwell, *On MSFT* offered advice, saying "Microsoft regularly patches Windows, as well, and it may be best to just wait for the next

official patch."

Important to note: Microsoft provided a statement. Contacted by *ZDNet* after the researcher dropped the zero-day on Twitter, Microsoft said this: "Windows has a customer commitment to investigate reported security issues, and proactively update impacted devices as soon as possible. Our standard policy is to provide solutions via our current Update Tuesday schedule."

Citation: Zero-day bug found in Windows 10, disclosed on Twitter (2018, October 25) retrieved 24 April 2024 from https://techxplore.com/news/2018-10-zero-day-bug-windows-disclosed-twitter.html