Exploit for wormable BlueKeep Windows bug released into the wild

Aurich Lawson

reader comments

33 with 23 posters participating, including story author

Share this story

For months, security practitioners have worried about the public release of attack code exploiting BlueKeep, the critical vulnerability in older versions of Microsoft Windows that's "wormable," meaning it can spread from computer to computer the way the WannaCry worm did two years ago. On Friday, that dreaded day arrived when the Metasploit framework—an open source tool used by white hat and black hat hackers alike—released just such an exploit into the wild.

The module, which was published as a work in progress on Github, doesn't yet have the polish and reliability of the EternalBlue exploit that was developed by the NSA and later used in WannaCry. For instance, if the people using the new module specify the wrong version of Windows they want to attack, they'll likely wind up with a blue-screen crash. Getting the exploit to work on server machines also requires a change to default settings in the form of a registry modification that turns on audio sharing.

By contrast, the wormable EternalBlue exploit—which a still-unidentified group calling itself the Shadow Brokers released

into the wild in April 2017—worked seamlessly against a wide range of Windows versions in their default settings. A month after the leak, EternalBlue was folded into the Wannacry ransomware worm that shut down computers worldwide. A month later, another EternalBlue-driven attack called NotPetya created still more worldwide destruction. The latest flaw, which is indexed as CVE-2019-0708 but is better known by the name BlueKeep, resides in earlier versions of the Remote Desktop Services, which help provide a graphical interface for connecting to Windows computers over the Internet. It affects Windows 2003 and XP, Vista 7, Server 2008 R2, and Server 2008. When Microsoft patched the vulnerability in May, it warned that computers that failed to install the fix could suffer a similar fate if reliable attack code ever becomes available. The reason: like the flaw that EternalBlue exploited, BlueKeep allowed for self-replicating attacks. Like a falling line of dominoes, a single exploit could spread from vulnerable machine to vulnerable machine with no interaction required of end users.

The risk was so great that Microsoft again implored customers to patch a month after its release. NSA officials also urged people to install the fix.

A big deal

As noted earlier, the module Metasploit developers released on Friday isn't quite as advanced as the leaked EternalBlue exploit, but it's still pretty effective. And that comes as both good and bad news for people who defend systems against malicious hacks.

"The release of this exploit is a big deal because it will put a reliable exploit in the hands of both security professionals and malicious actors," Ryan Hanson, principal research consultant at Atredis Partners and a developer who helped work on the release, told Ars. "I'm hoping the exploit will be

primarily used by offensive teams to demonstrate the importance of security patches, but we will likely see criminal groups modifying it to deliver ransomware as well."

He continued:

> *It's not very often that you see Microsoft release a warning like they did with this bug. I'm sure the warning caused defensive teams to be more diligent about ensuring that all vulnerable systems were patched quickly, which was the purpose of the warning. However, Microsoft's warning was more of a "Capture the Flag" challenge for those of us on the offensive side. I rarely reverse security patches, but I became very curious and decided to reverse the patch as a learning exercise and also to figure out why Microsoft considered this bug to be so dangerous. Only a few days after the patch, people started sharing proof they had already reversed the patch and triggered a crash. Not long after, proof of successful code execution was shared by multiple people, including myself.*
>
> *Although several people had publicly proven code execution, nobody released their PoCs, which I assume is because we all realized exactly why Microsoft warned everyone about the dangers of this bug. Shortly after people started showing proof of code execution, the NSA also released an advisory regarding the risks associated with BlueKeep. With all the warnings and risks associated with this bug, it is pretty significant that an exploit will be released publicly for the first time. Especially after so many researchers have kept their PoCs private.*

A single machine is all it takes

Another of the primary developers behind the release is Sean Dillon, a senior security researcher at RiskSense. Friday's release is almost identical to the BlueKeep exploit video he

published in June. It showed the module connecting to an unpatched Windows Server 2008 R2 computer, and using the exploit, had highly privileged System privileges. Dillon then used the open source Mimikatz application to obtain the cryptographic hashes of passwords belonging to other computers on the same network the hacked machine was connected to.

The ability to dump credentials used to connect to other computers underscores a key danger posed by the vulnerability. A single vulnerable machine could be used to infect all other machines in a network even if they're fully up to date. Dillon's video graphically portrayed this threat in June. With the open source code now available for anyone to examine, rewrite, or repurpose, the risk will be even harder for people to ignore.

"As an open-source project, one of Metasploit's guiding principles is that knowledge is most powerful when shared," s Brent Cook, the Metasploit engineering manager at security firm Rapid7 wrote in a post published on Friday. "Democratic access to attacker capabilities, including exploits, is critical for defenders—particularly those who rely on open-source tooling to understand and effectively mitigate risk."

https://arstechnica.com/?p=1563639