rkt Container Runtime Flaws Give Root Access to Host

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/K2ajf7Gb1kI/rkt-container-runtime-flaws-give-root-access-host

---

Microsoft practically begs Windows users to fix wormable BlueKeep flaw



Aurich Lawson

reader comments

49 with 30 posters participating

Share this story

Microsoft security officials say they are confident an exploit exists for BlueKeep, the recently patched vulnerability that has the potential to trigger self-replicating attacks as destructive as the 2017 WannaCry attack that shut down computers all over the world.

In a Blog post published late Thursday night, members of the Microsoft Security Response Center cited findings published Tuesday by Errata Security CEO Rob Graham that almost 1 million Internet-connected computers remain vulnerable to the attacks. That indicates those machines have yet to install an update Microsoft issued two weeks ago patching against the so-called BlueKeep vulnerability, which is formally tracked as CVE-2019-0708. The exploits can reliably execute malicious code with no interaction on the part of an end user. The severity prompted Microsoft to take the unusual step of issuing patches for Windows 2003, XP, and Vista, which haven't been supported in four, five, and two years, respectively.

Thursday's post warned, once again, that the inaction could trigger another worm of the magnitude of WannaCry, which caused hospitals to turn away patients and paralyzed banks, shipping docks, and transportation hubs around the world. In Thursday's post MSRC officials wrote:

> *Microsoft is confident that an exploit exists for this vulnerability, and if recent reports are accurate, nearly one million computers connected directly to the internet are still vulnerable to CVE-2019-0708. Many more within corporate networks may also be vulnerable. It only takes one vulnerable computer connected to the internet to provide a potential gateway into these corporate networks, where advanced malware could spread, infecting computers across the enterprise. This scenario could be even worse for those who have not kept their internal systems updated with the latest fixes, as any future malware may also attempt further exploitation of*

vulnerabilities that have already been fixed.

Microsoft reminded people that WannaCry wasn't unleashed until two months after the release of MS17-010, the update that patched the vulnerability exploited by WannaCry. It resided in SMBv1, an early version of the server message block protocol that allows one computer to share files and directories with other computers. Security experts use the word "wormable" to describe the vulnerability because of its ability to trigger worms, which are self-replicating attacks that require no interaction on the part of end users. The wormable BlueKeep flaw, by contrast, stems from a "dangling pointer" bug in the Remote Desktop Protocol, which provides a graphical interface for connecting to another computer over the Internet.

Of course, the big difference two years ago was the public release of Eternal Blue, an exploit that was developed by, and later stolen from, the National Security Agency, which is arguably the world's most advanced hacking organization. A still unidentified group calling itself the Shadow Brokers published Eternal Blue in April, 2017. The release provided even inexperienced hackers the world over with an easy way to reliably force vulnerable computers to execute code of their choice. A month later, the WannaCry worm repurposed Eternal Blue and ended up infecting computers all over the world in a matter of hours.

This time around, there has been no public release of code exploiting BlueKeep, although a handful of white hat hackers have reported independently developing exploits that they say are every bit as wormable as Microsoft has warned. It's not clear precisely what MSRC officials meant when they wrote they are "confident that an exploit exists for this vulnerability." They may be referring to the same white hat hackers described above. Or, they may be referring to more nefarious actors. Ars asked Microsoft for more details and will update this post if their representatives provide them.

Microsoft is urging anyone who is running a vulnerable computer to update at once. The flaw affects versions from Windows XP through Server 2008 R2. Anyone using one of these versions should ensure a patch is in place. They should also test to make sure RDP is not exposed to the Internet unless absolutely necessary. Enabling Network Level Authentication for remote desktop services is a helpful measure, but it’s ineffective against attackers who have network passwords, which is a common occurrence in ransomware infections. Windows 8 and 10 are unaffected.

https://arstechnica.com/?p=1513201

Microsoft Reminds Users to Patch Wormable ‘BlueKeep’ Vulnerability

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/JGDwh5MgUv8/microsoft-reminds-users-patch-wormable-bluekeep-vulnerability

---

High-Risk Flaws Found in

Process Control Systems From B&R Automation

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/t0W0IeYgqMQ/high-risk-flaws-found-process-control-systems-br-automation

---

Apple Patches SQLite, WebKit Bugs in iTunes and iCloud for Windows

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/OagdbICaLow/apple-patches-sqlite-webkit-bugs-itunes-and-icloud-windows

---

Docker Vulnerability Gives Arbitrary File Access to Host

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_2Du85DLyPU/docker-vulnerability-gives-arbitrary-file-access-host

Google Researcher Finds Code Execution Vulnerability in Notepad

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bg5brXT12eQ/google-researcher-finds-code-execution-vulnerability-notepad

---

One Million Devices Vulnerable to BlueKeep as Hackers Scan for Targets

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/qpNPyk04hAU/one-million-devices-vulnerable-bluekeep-hackers-scan-targets

---

Siemens Medical Products

Affected by Wormable Windows Flaw

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4BfvQgZRcq4/siemens-medical-products-affected-wormable-windows-flaw

---

GitHub Adds New Tools to Help Developers Secure Code

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Sjd-5-SbsV4/github-adds-new-tools-help-developers-secure-code