Hackers Corner
CVE-2019-0708 (BlueKeep)

Background

Patch Tuesday is an unofficial term used to refer to Microsoft's regular release of security updates for its products. On May 14, 2019, Patch Tuesday included 79 vulnerabilities in an update from Microsoft. Of the 79 vulnerabilities, 22 of them were labeled as critical, four of those being remote code execution attacks.

This Microsoft update quickly gained media attention amidst a flurry of other releases that included several updates from Adobe, a processor exploit called Zombieload[i], a buffer overflow in WhatsApp[ii] and 😾😾😾, also known as Thrangrycat[iii], affecting Cisco Products. The reason why this Microsoft update[iv] generated so much attention is due to warnings about a specific vulnerability, CVE-2019-0708[v], a remote code execution vulnerability in Microsoft's remote desktop protocol. Microsoft noted in their update that this vulnerability is wormable and presents a risk similar to WannaCry[vi], NotPetya[vii], and BadRabbit[viii].

Event

CVE-2019-0708, named BlueKeep, is a vulnerability what was publicly disclosed during Microsoft's Patch Tuesday in May. Microsoft in-support systems that are vulnerable to this attack include Windows 7, Windows Server 2008, and Windows Server 2008 R2. This potential impact from this disclosure was severe enough that Microsoft even released an update for out-of-support systems impacted by the vulnerability. These systems included Windows 2003 and Windows XP.

As Microsoft has warned, this vulnerability requires no user interactions and is wormable. A system is simply exploited by sending a specially crafted request to a remote Windows instance. The exploit abuses how Remote Desktop Services handle the connection request. Several proofs-of-concepts for the exploit now exist, but there are no active campaigns as of this moment.

Microsoft and researchers over the past several weeks have been advising users and corporations about this vulnerability and the possibility of a significant event in the coming months. Many parallels have also been drawn to the events that unfolded after Microsoft released MS17-010[ix], the update that patched a vulnerability in Windows that would be exploited by WannaCry two months later.

Insight

At the moment, these are all just warnings from the Microsoft/security community in combination with patches and updates from Microsoft. Corporations need to take inventory and understand which devices they have on their networks so they can maintain and patch them.

In this case, researchers and vendors were able to get in front of a possible campaign. The only thing left standing between cybercriminals and your network is proper security hygiene. Corporations, both large and small, must enforce timely updates and system patches when vulnerabilities are disclosed.

Patch Tuesday is the second and fourth Tuesday of every month.

Advice

It's advised that corporations apply patches and update all systems, including those that are out of support. If your devices are out of support, consider upgrading. The second piece of advice comes from researcher Robert Graham's blog, *Almost One Million Vulnerable to BlueKeep Vuln*[x], where he details a more critical problem that needs to be addressed inside corporate environments: psexec, a versatile Windows command line tool that lets you run processes on remote systems with local user credentials.

"You may have only one old WinXP machine that's vulnerable, that you don't care if it gets infected with ransomware. But, that machine may have a Domain Admin logged in, so that when the worm breaks in, it grab those credentials and uses them to log onto the Domain Controller. Then, from the Domain Controller, the worm sends a copy of itself to all the desktop and servers in the organization, using those credentials instead of the vuln. This is what happened with notPetya: the actual vulnerability wasn't the problem, it was psexec that was the problem."

Under Attack and in Need of Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://zombieloadattack.com/
[ii] https://nvd.nist.gov/vuln/detail/CVE-2019-3568
[iii] https://thrangrycat.com/
[iv] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[v] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
[vi] https://security.radware.com/ddos-threats-attacks/wannacry-ransomware/
[vii] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/petya-petrwrap/
[viii] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/badrabbit/
[ix] https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
[x] https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XPVAANNKja4