kindred

Security Newsletter

10 June 2019

Subscribe to this newsletter

Nearly 1 Million Computers Still Vulnerable to "Wormable" BlueKeep RDP Flaw

Nearly 1 million Windows systems are still unpatched and have been found vulnerable to a recently disclosed critical, wormable, remote code execution vulnerability in the Windows Remote Desktop Protocol (RDP)—two weeks after Microsoft releases the security patch. If exploited, the vulnerability could allow an attacker to easily cause havoc around the world, potentially much worse than what WannaCry and NotPetya like wormable attacks did in 2017.

Dubbed BlueKeep and tracked as CVE-2019-0708, the vulnerability affects Windows 2003, XP, Windows 7, Windows Server 2008 and 2008 R2 editions and could spread automatically on unprotected systems. The BlueKeep vulnerability has so much potential to wreak havoc worldwide that it forced Microsoft to release patches for not only the supported Windows versions but also Windows XP, Windows Vista and Windows Server 2003, which no longer receive mainstream support from the company but are still widely used.

If fixing the flaw in your organisation is not possible anytime sooner, then you can take these mitigations: Disable RDP services, if not required. Block port 3389 using a firewall or make it accessible only over a private VPN. Enable Network Level Authentication (NLA) – this is partial mitigation to prevent any unauthenticated attacker from exploiting this Wormable flaw.

Read More on TheHackerNews

GoldBrute Botnet Brute-Force Attacking 1.5M RDP Servers

While the end-goal of the group controlling the botnet is not clear, it appears that GoldBrute is currently using brute-force methods to attack about 1.5 million Remote Desktop Protocol servers that have exposed connections to the open internet.

A scan using the Shodan search engine shows that there are at least 2.4 million of these exposed Remote Desktop Protocol servers throughout the world. GoldBrute, however, seems to use its own list as part of the attacks and keeps expanding as that list grows.

While there is not an immediate connection between BlueKeep and GoldBrute, it doesn't mean that the group controlling the botnet could not use that vulnerability in the future.

Read More on BankInfoSecurity

More #News

- For two hours, a large chunk of European mobile traffic was rerouted through China
- Microsoft warns about email spam campaign abusing Office vulnerability
- From phish to network compromise in two hours: How Carbanak operates
- macOS Catalina Brings Several Security Improvements
- Only 5.5% of all vulnerabilities are ever exploited in the wild
- Google may limit ad blockers for Chrome users
- Headhunting Firm Leaks Millions of Resumes, Client Private Data
- Phishing attacks that bypass 2-factor authentication are now easier to execute
- 8.4TB in email metadata exposed in university data leak
- Cryptocurrency attack thwarted by npm team

- Cryptocurrency attack thwarted by npm team
- The clever cryptography behind Apple's "Find My" feature.
- 19 Cases of Insider Bank Threats
- The SIM Swapping Bible: What To Do When SIM-Swapping Happens To You

#Patch Time!

- VLC 3.0.7 is Biggest Security Release Due to EU Bounty Program
- Major HSM vulnerabilities impact banks, cloud providers, governments
- NVIDIA Fixes High Severity GeForce Experience Vulnerabilities
- New Windows 10 Zero-Day Bug Emerges From Bypassing Patched Flaw
- Action required! Exim mail servers need urgent patching
- VMware Patches Vulnerabilities in Tools, Workstation
- Cisco Fixes High Severity Flaws in Industrial, Enterprise Tools
- Patch Android! June 2019 update fixes eight critical flaws
- Unpatched Bug Let Attackers Bypass Windows Lock Screen On RDP Sessions
- macOS 0-Day Flaw Lets Hackers Bypass Security Features With Synthetic Clicks
- Apple Emphasizes Privacy With Single Sign-On Feature

#Tech and #Tools

- Sysmon Getting DNS Query Logging with Querying Process Name
- Two-thirds of iOS apps disable ATS, an iOS security feature
- Large European Routing Leak Sends Traffic Through China Telecom
- Liffy: Local file inclusion exploitation tool
- A walkthrough on how to set up and use BloodHound
- ArchStrike: An Arch Linux repository for security professionals and enthusiasts
- Osquery for Windows access right misconfiguration Elevation of Privilege (CVE-2019-3567)
- H8mail: Password breach hunting tool
- WAF through the eyes of hackers
- Bypassing CSP with policy injection
- SameSite Cookies in practice
- Kerberos (II): How to attack Kerberos?
- SecDevLab: A laboratory for effectively learning secure web development.
- CVE-2019-0708 (BlueKeep) PoC
- Using osquery for remote forensics
- Passive DNS - a tutorial to setup your own Passive DNS using D4 Project
- Pesky Old-Style Macro Popups — Advanced Maldoc Techniques
- Bypass AppLocker default rules
- Using Sysmon in Azure Sentinel
- Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us