LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing Remote Desktop Protocol Exploitation

OVERALL CLASSIFICATION IS

TLP:WHITE

November 21, 2019

Agenda

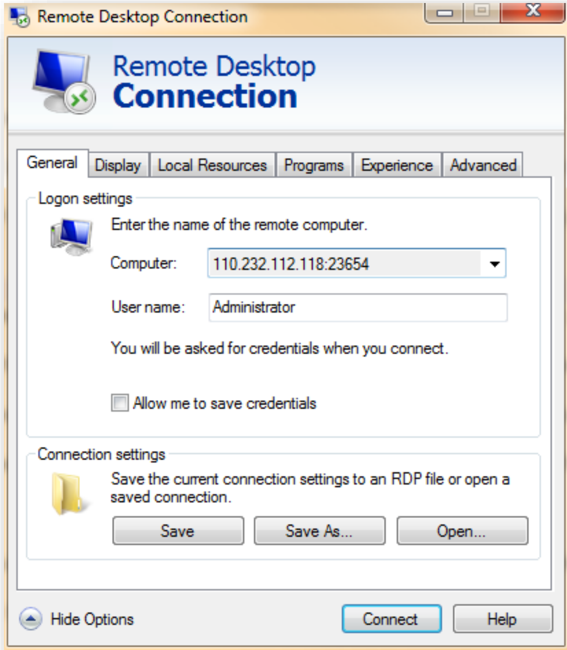
- Overview
- History
- Usage
- Maturity of RDP implementation
- Why does RDP matter to healthcare cybersecurity?
- RDP Exploitation
- Major exploits: Bluekeep and DejaBlue
- RDP Threats – who and what attacks RDP?
- Securing RDP
- References
- Questions

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- Proprietary protocol, originally developed by Microsoft
- Formerly known as Terminal Services Client
  - Introduced in Windows NT 4.0 (1996)
  - Became part of Remote Desktop Services (RDS) in 2009
- Implementations currently exist for Windows, Unix, Linux, Mac, iOS and Android, etc…
- Legitimate use for remote access for IT support:
  - Administration
  - Maintenance
  - Troubleshooting
  - User assistance
- Utilizes TCP and UDP ports 3389 by default
- Highly vulnerable to attack
  - Remote access is desired by hackers
- Frequently exploited by many vulnerabilities and tactics



Logon settings

Enter the name of the remote computer.

Computer: 110.232.112.118:23654

User name: Administrator

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Image courtesy of Mammoth.com.au

History

The evolution of RDP:

RDP VERSION	WINDOWS OS	NOTES
4	Win NT 4.0	First version of RDP, Based on the ITU-T T.128 application sharing protocol; introduced with terminal services
5	Win 2000 Server	Support for printing; improved bandwidth usage
5.1	Windows XP	Support for 24-bit color and sound; Client available for Windows 2000, Windows 95/98 and Windows NT 4.0.; Name of the client changed from Terminal Services Client to Remote Desktop Connection
5.2	Windows server 2003	Support for console mode connections, session directory, and local resource mapping; Transport Layer Security (TLS) available for authentication and encryption with server
6	Windows Vista	Multi-monitor spanning and large desktop support
6.1	Windows Server 2008, Windows Vista Service Pack 1, Windows XP Service Pack 3	Support for connecting remotely to individual programs
7	Windows Server 2007 R2, Windows 7	Renamed Terminal Services to Remote Desktop Services
7.1	Windows 7 Service Pack 1, Windows 2008 R2 Service Pack 1	
8	Windows 8, Windows Server 2012	Automatic selection of TCP or UD; Adaptive Graphics; multi touch support
8.1	Windows 8.1, Windows Server 2012 R2	Support for session shadowing
10	Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2	AutoSize zoom

Usage

- Most current RDP implementations allow for:
  - Windows Presentation Foundation (WPF) applications and remoting
  - Clipboard sharing between a remote server and a local client
  - Remote desktop applications execution on client machines
  - Aeroglass remoting
  - Windows Media Player (WMP) redirection
  - Implementation on non-Microsoft platforms
    - e.g. Unix/Linux platforms use rdesktop
  - Mouse and user keyboard data encryption
  - Audio, printer, port and file redirection
  - Multiple monitor support

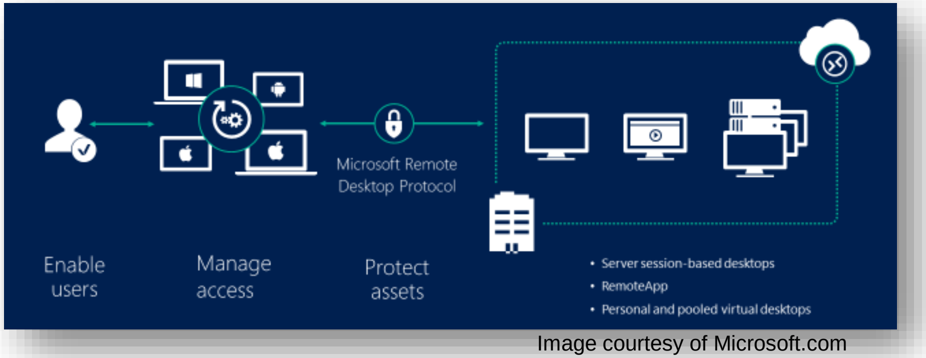

Microsoft Remote Desktop Protocol
Enable users
Manage access
Protect assets
Server session-based desktops
RemoteApp
Personal and pooled virtual desktops

Image courtesy of Microsoft.com

TLP:WHITE

Maturity of RDP implementation

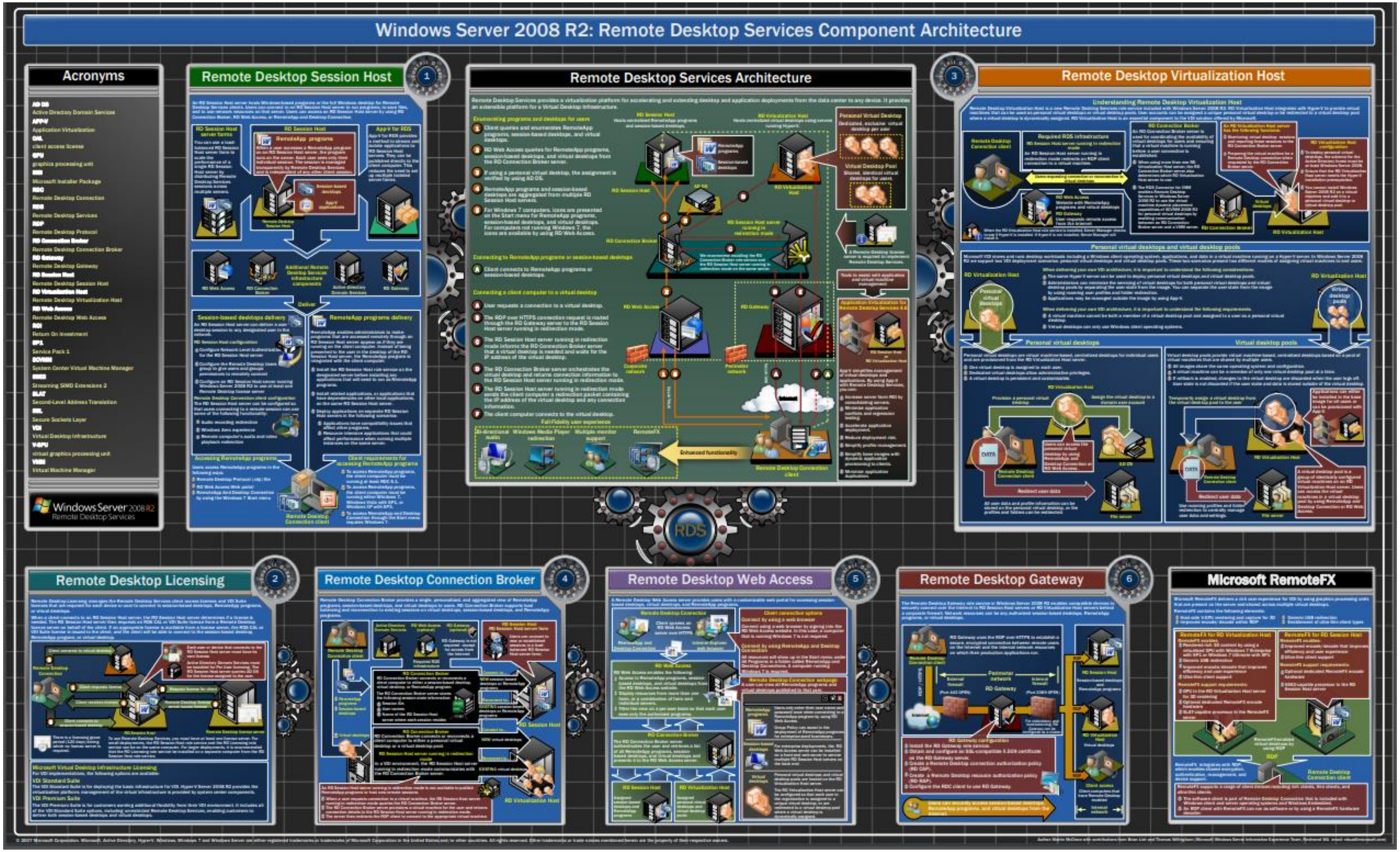
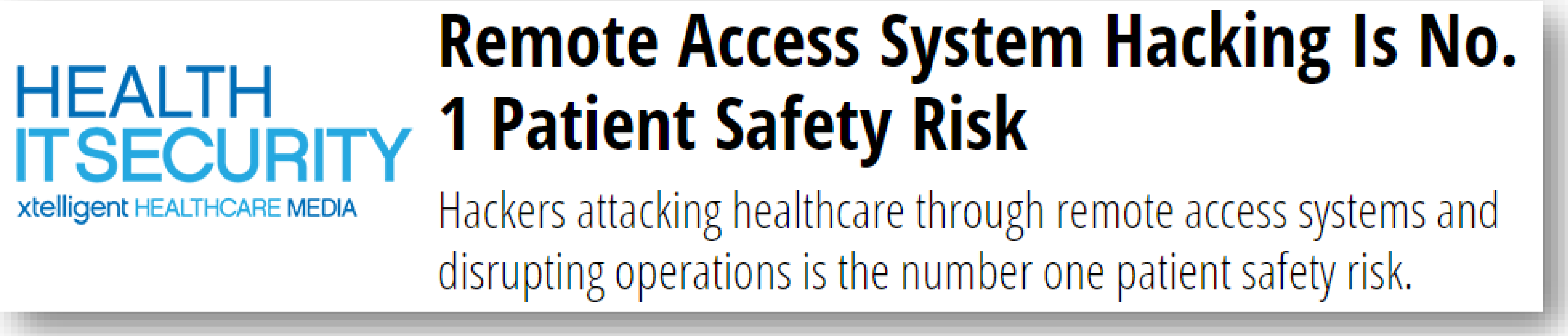

Windows Server 2008 R2: Remote Desktop Services Component Architecture
Acronyms
Remote Desktop Session Host
1
Remote Desktop Services Architecture
3
Remote Desktop Virtualization Host
Windows Server 2008 R2
Remote Desktop Services
RDS
Remote Desktop Licensing
2
Remote Desktop Connection Broker
4
Remote Desktop Web Access
5
Remote Desktop Gateway
6
Microsoft RemoteFX

Image courtesy of Microsoft.com

Why does RDP matter to healthcare cybersecurity?

- Targeting
  - ECRI Institute’s annual Top 10 Health Technology Hazards for 2019
    - Hackers attacking healthcare through remote access systems and disrupting operations is the number one patient safety risk
  - Oleg Kolesnikov, Head of Securonix Threat Research Labs, Referring to RDP:
    - “…if it’s targeted, particularly in healthcare, and exploited, the results can be much more severe…”
  - Trapx Securty:
    - “One of the most common breach scenarios, whether by an insider (a rogue employee) or by an external attacker who has successfully breached the perimeter, happens through RDP.”

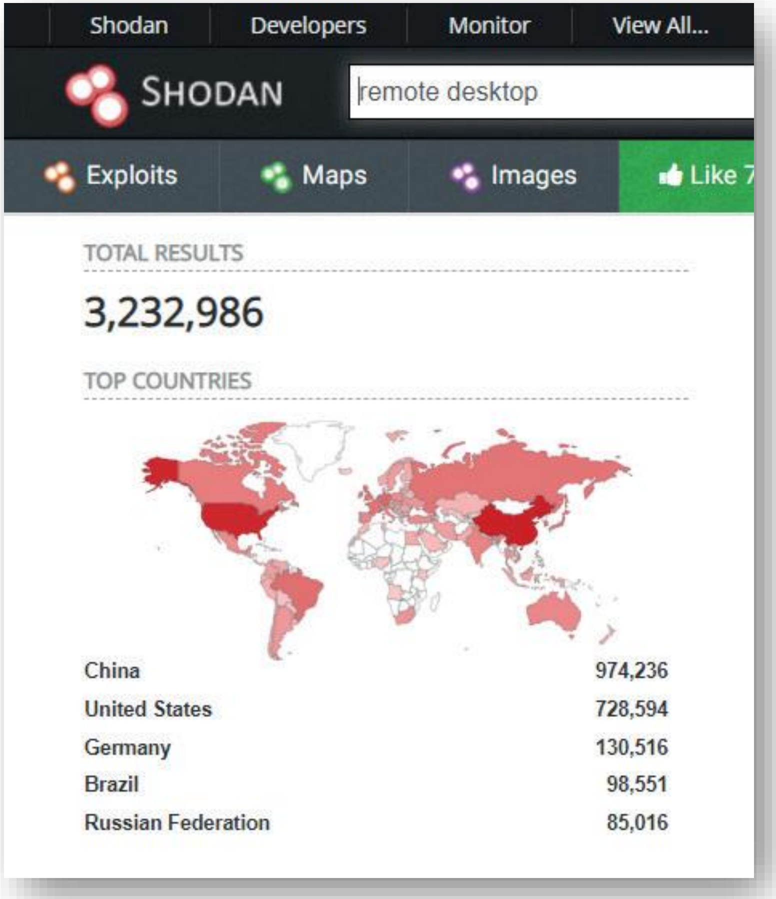


Remote Access System Hacking Is No. 1 Patient Safety Risk

Hackers attacking healthcare through remote access systems and disrupting operations is the number one patient safety risk.

RDP exploitation

- Sophos leveraged Shodan to assess global RDP vulnerabilities:



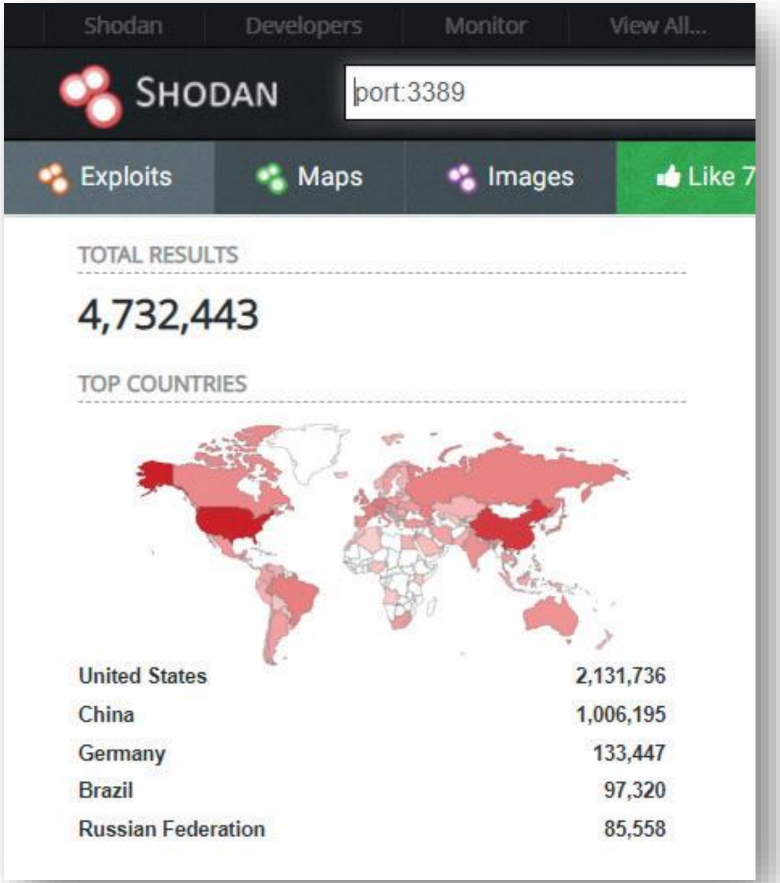
remote desktop

TOTAL RESULTS

3,232,986

TOP COUNTRIES

China	974,236
United States	728,594
Germany	130,516
Brazil	98,551
Russian Federation	85,016



port:3389

TOTAL RESULTS

4,732,443

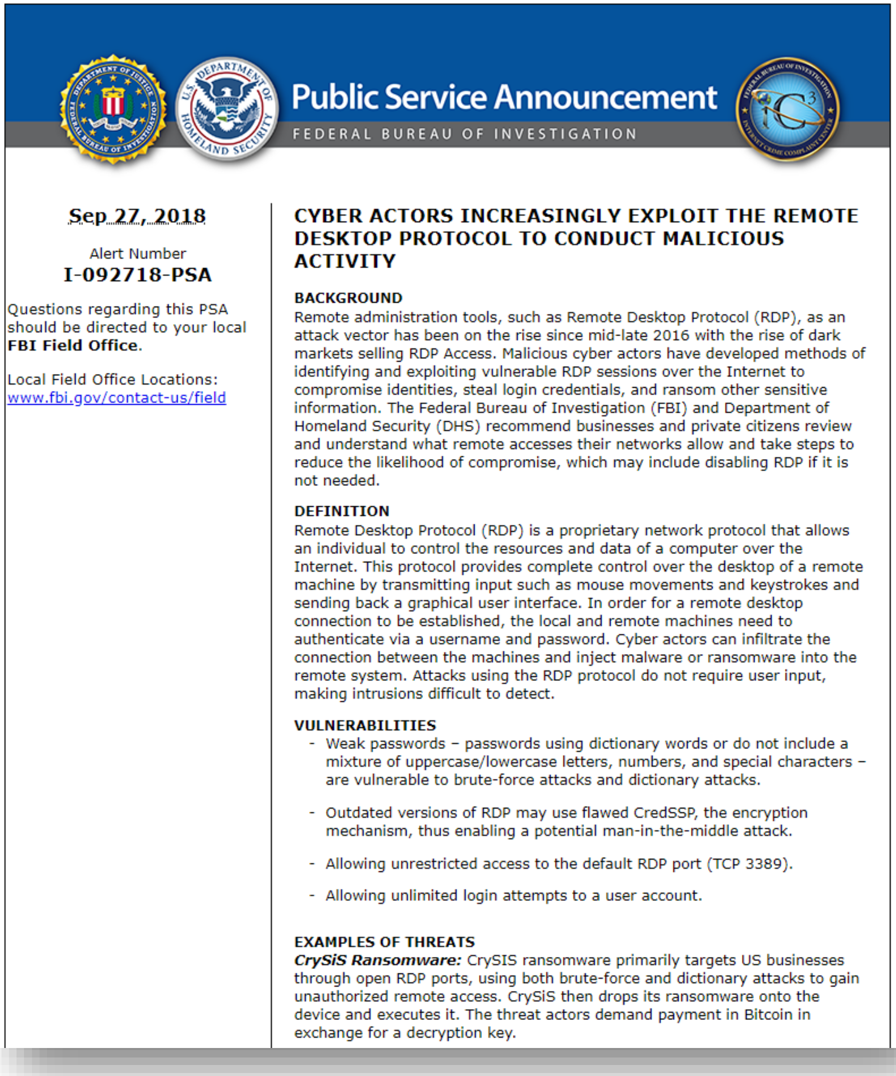
TOP COUNTRIES

United States	2,131,736
China	1,006,195
Germany	133,447
Brazil	97,320
Russian Federation	85,558

RDP is already being abused, every day, to devastating effect. - Sophos

RDP exploitation (continued)

- FBI released RDP PSA in September 2018:
  - "…as an attack vector on the rise since mid-late 2016…"
  - Frequently for sale on the dark web
  - Used to:
    - Compromise identities
    - Steal login credentials
    - Demand ransom (ransomware)
    - Steal other sensitive information
  - Vulnerabilities:
    - Weak passwords
    - Outdated installations
    - Unrestricted RDP access
    - Unlimited authentication attempts
  - Threats: CrySiS, CryptON, Samsam
  - Defense: Auditing, 2FA, logging, etc…



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Sep 27, 2018

Alert Number
I-092718-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

CYBER ACTORS INCREASINGLY EXPLOIT THE REMOTE DESKTOP PROTOCOL TO CONDUCT MALICIOUS ACTIVITY

BACKGROUND
Remote administration tools, such as Remote Desktop Protocol (RDP), as an attack vector has been on the rise since mid-late 2016 with the rise of dark markets selling RDP Access. Malicious cyber actors have developed methods of identifying and exploiting vulnerable RDP sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) recommend businesses and private citizens review and understand what remote accesses their networks allow and take steps to reduce the likelihood of compromise, which may include disabling RDP if it is not needed.

DEFINITION
Remote Desktop Protocol (RDP) is a proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet. This protocol provides complete control over the desktop of a remote machine by transmitting input such as mouse movements and keystrokes and sending back a graphical user interface. In order for a remote desktop connection to be established, the local and remote machines need to authenticate via a username and password. Cyber actors can infiltrate the connection between the machines and inject malware or ransomware into the remote system. Attacks using the RDP protocol do not require user input, making intrusions difficult to detect.

VULNERABILITIES

- Weak passwords – passwords using dictionary words or do not include a mixture of uppercase/lowercase letters, numbers, and special characters – are vulnerable to brute-force attacks and dictionary attacks.
- Outdated versions of RDP may use flawed CredSSP, the encryption mechanism, thus enabling a potential man-in-the-middle attack.
- Allowing unrestricted access to the default RDP port (TCP 3389).
- Allowing unlimited login attempts to a user account.

EXAMPLES OF THREATS
CrySiS Ransomware: CrySIS ransomware primarily targets US businesses through open RDP ports, using both brute-force and dictionary attacks to gain unauthorized remote access. CrySiS then drops its ransomware onto the device and executes it. The threat actors demand payment in Bitcoin in exchange for a decryption key.

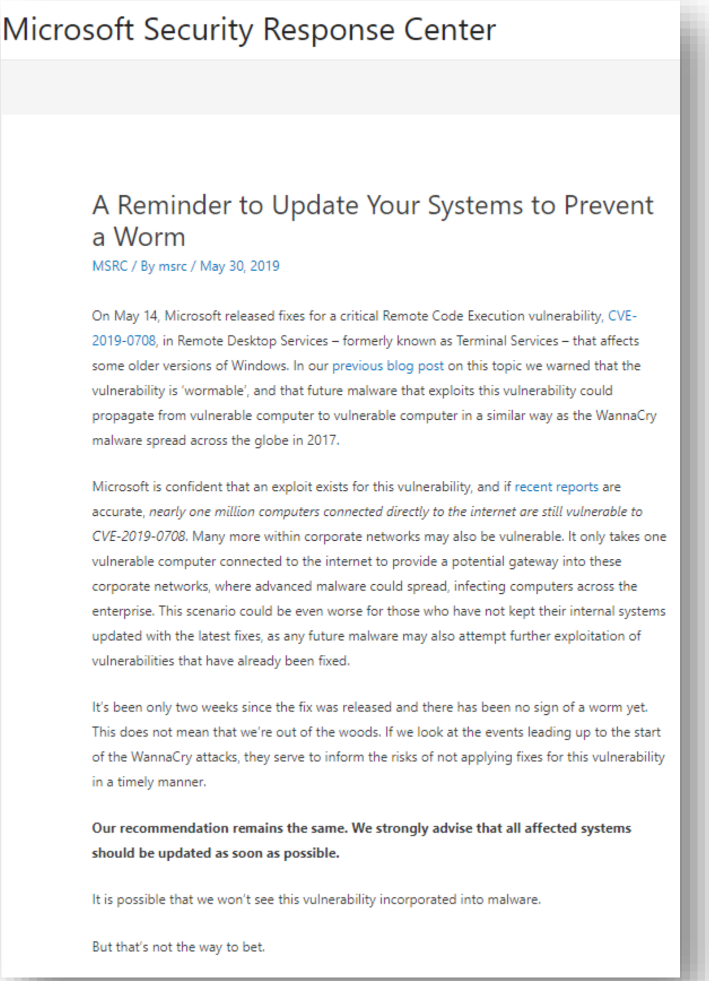
Major exploits: Bluekeep and DejaBlue

Image courtesy of Medium.com

- BlueKeep (and related vulnerabilities)
  - Target Microsoft Windows
    - Windows XP
    - Windows Server 2003
    - Windows Vista
    - Windows 7
    - Windows Server 2008
    - Windows 10
  - CVE-2019-0708 (Bluekeep)
    - CVE-2019-1181, CVE-2019-1182 (Dejablue)
  - Remote Code execution
  - “Wormable”
  - Microsoft Bluekeep severity categorization: Critical
  - Microsoft released patch for Bluekeep in May of 2019, Dejablue in Oct. 2019
    - Two weeks after Bluekeep patch was released, one researcher noted almost 1M systems still remained unpatched
  - NSA released Bluekeep warning

Major exploits: Bluekeep and DejaBlue (continued)

- Microsoft and NSA Bluekeep releases:



Microsoft Security Response Center

A Reminder to Update Your Systems to Prevent a Worm

MSRC / By msrc / May 30, 2019

On May 14, Microsoft released fixes for a critical Remote Code Execution vulnerability, CVE-2019-0708, in Remote Desktop Services – formerly known as Terminal Services – that affects some older versions of Windows. In our previous blog post on this topic we warned that the vulnerability is 'wormable', and that future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017.

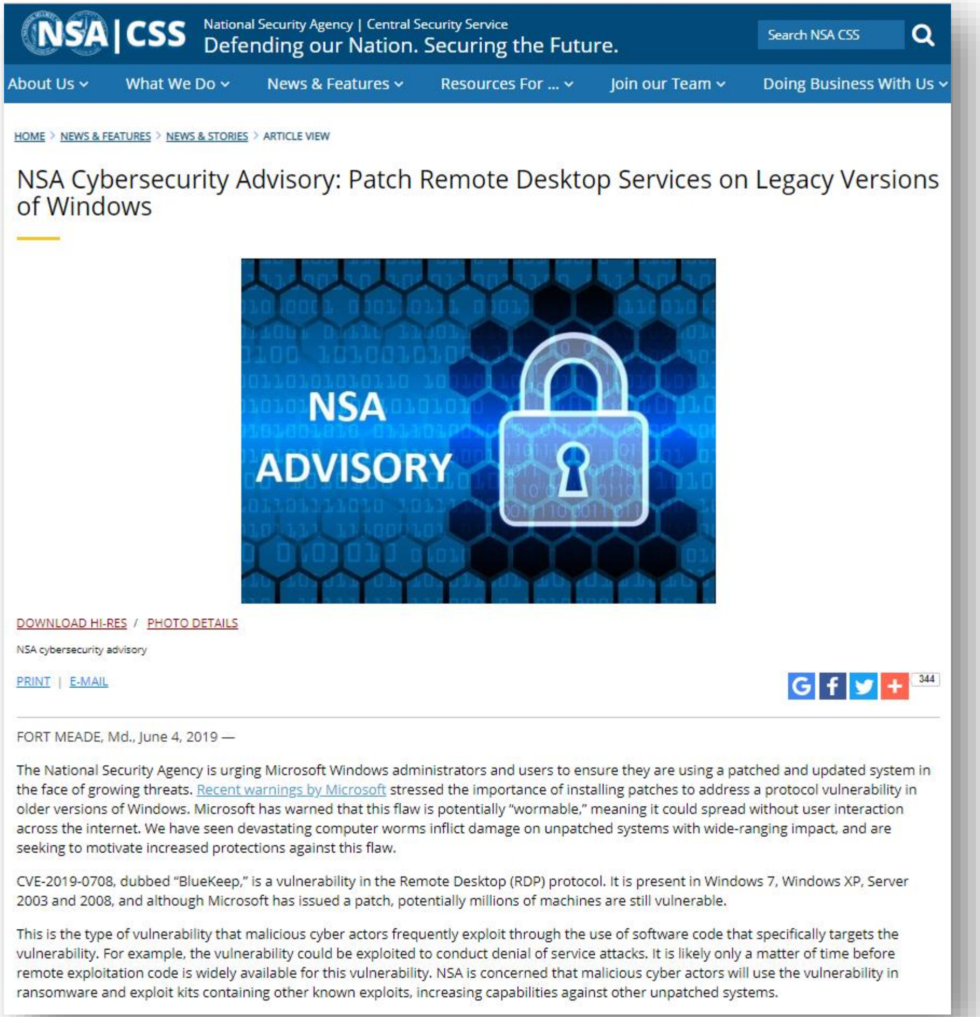
Microsoft is confident that an exploit exists for this vulnerability, and if recent reports are accurate, *nearly one million computers connected directly to the internet are still vulnerable to CVE-2019-0708*. Many more within corporate networks may also be vulnerable. It only takes one vulnerable computer 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.

It's been only two weeks since the fix was released and there has been no sign of a worm yet. This does not mean that we're out of the woods. If we look at the events leading up to the start of the WannaCry attacks, they serve to inform the risks of not applying fixes for this vulnerability in a timely manner.

Our recommendation remains the same. We strongly advise that all affected systems should be updated as soon as possible.

It is possible that we won't see this vulnerability incorporated into malware.

But that's not the way to bet.



NSA|CSS
National Security Agency | Central Security Service
Defending our Nation. Securing the Future.
Search NSA CSS
About Us
What We Do
News & Features
Resources For ...
Join our Team
Doing Business With Us
HOME > NEWS & FEATURES > NEWS & STORIES > ARTICLE VIEW
NSA
ADVISORY
DOWNLOAD HI-RES / PHOTO DETAILS
PRINT | E-MAIL
344

NSA Cybersecurity Advisory: Patch Remote Desktop Services on Legacy Versions of Windows

NSA cybersecurity advisory

FORT MEADE, Md., June 4, 2019 —

The National Security Agency is urging Microsoft Windows administrators and users to ensure they are using a patched and updated system in the face of growing threats. Recent warnings by Microsoft stressed the importance of installing patches to address a protocol vulnerability in older versions of Windows. Microsoft has warned that this flaw is potentially "wormable," meaning it could spread without user interaction across the internet. We have seen devastating computer worms inflict damage on unpatched systems with wide-ranging impact, and are seeking to motivate increased protections against this flaw.

CVE-2019-0708, dubbed "BlueKeep," is a vulnerability in the Remote Desktop (RDP) protocol. It is present in Windows 7, Windows XP, Server 2003 and 2008, and although Microsoft has issued a patch, potentially millions of machines are still vulnerable.

This is the type of vulnerability that malicious cyber actors frequently exploit through the use of software code that specifically targets the vulnerability. For example, the vulnerability could be exploited to conduct denial of service attacks. It is likely only a matter of time before remote exploitation code is widely available for this vulnerability. NSA is concerned that malicious cyber actors will use the vulnerability in ransomware and exploit kits containing other known exploits, increasing capabilities against other unpatched systems.

RDP Threats – who and what attacks RDP?

Ransomware

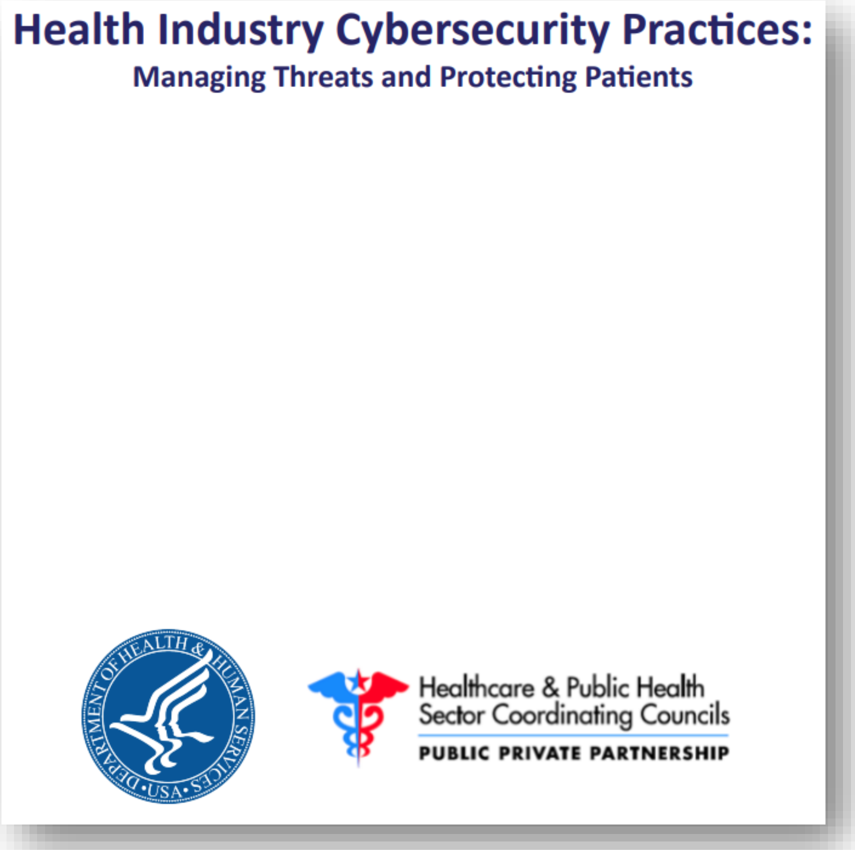
- Apocalypse
- CrySiS/Dharma
- CryptON
- Samsam (Samas)
- Ryuk
- Sodinokibi
- SynAck
- DMA Locker
- LockCrypt
- Scarabey
- Horsuke
- Bit Paymer
- RSAUtil
- Xpan
- LowLevel
- Smrss32
- WannaCry
- Aura/BandarChor
- ACCDFISA
- Globe
- And more…

Threat Actors

- APT1
- APT3
- APT39
- APT41
- Axiom
- Carbanak
- Cobalt Group
- Cobalt Strike
- DarkComet
- Dragonfly 2.0
- FIN10
- FIN6
- FIN8
- jRAT
- Koadic
- Lazarus Group
- Leviathan
- menuPass
- njRAT
- OilRig
- Patchwork
- Pupy
- QuasarRAT
- Revenge RAT
- ServHelper
- Stolen Pencil
- TEMP.Veles
- zwShell/ZxShell
- And more…

Securing RDP

- Recommended cybersecurity defense and response practices:



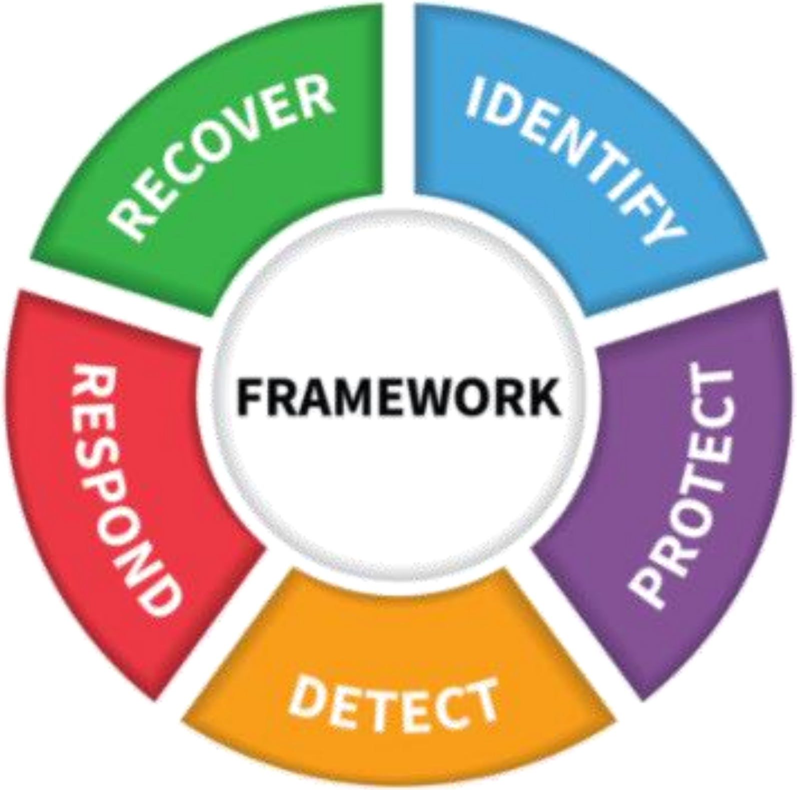
Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

405(d) HICP



NIST Cybersecurity Framework

Securing RDP (continued)

405(d) cybersecurity practice references denoted in red

- Specific steps for securing RDP
  - Whenever possible on Windows implementation, use group policy object (GPO) functionality to centrally manage RDP [3.S.A], [3.L.B]
  - Use strong/complex passwords; require periodic password changes [3.S.A], [3.M.C], [3.L.C]
    - Letters, numbers, symbols and password length minimums
    - Balance between password change window that is too long and too short
  - Restrict access using firewalls [3.S.A], [3.M.C], [3.L.C]
    - Filter via IP address, MAC address, etc…
  - Reassign RDP to another port (change listening port from default 3389) [6.M.A]
  - Update software; Apply patches [7.S.A], [7.M.D]
    - Patch management program

RDP Stands for "Really DO Patch!"

McAfee.com

Securing RDP (continued)

405(d) cybersecurity practice references denoted in red

- Specific steps for securing RDP (continued)
  - Use RDP gateway [6.S.A], [6.M.B], [6.L.A]
    - Funnell remote connections through a single “gateway" server
  - Tunnel Remote Desktop connections through IPSec or SSH [4.S.A], [4.M.C], [4.L.A]
    - Alternate to RDP gateway
  - Set restrictions on accounts [3.S.A], [3.M.A], [3.L.C]
    - Enable network-level authentication
      - Additional layer of authentication
    - Implement two-factor authentication
    - Limit RDP usage to only those whose role absolutely requires it
    - Implement RDP account lockout policy
    - Implement auto-disable for accounts that are not used after set period of time
    - Log and review all RDP access
      - On Windows system, domain controller can audit
      - Firewall logs

References

- How to change the listening port for Remote Desktop, Microsoft Support, 8/13/2018, https://support.microsoft.com/en-us/help/306759/how-to-change-the-listening-port-for-remote-desktop
- Fitzpatrick, Darren, Fokker, John and Ryan, Eamonn, RDP Security Explained, McAfee Labs, 6/24/2019, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-security-explained/
- InfoSec Guide: Remote Desktop Protocol (RDP), Trend Micro, October 31, 2018, Trend Micro, 10/31/2018, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/infosec-guide-remote-desktop-protocol-rdp
- Camp, Cameron, Remote Desktop (RDP) Hacking 101: I can see your desktop from here!, ESET - We Live Security, 9/16/2013, https://www.welivesecurity.com/2013/09/16/remote-desktop-rdp-hacking-101-i-can-see-your-desktop-from-here/
- Definition of: Terminal Services, PC Mag Encyclopedia, https://www.pcmag.com/encyclopedia/term/52755/terminal-services
- Alert #: I-092718-PSA - Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity, Federal Bureau of Investigation Public Service, https://www.ic3.gov/media/2018/180927.aspx
- Greenberg, Andy, DejaBlue: New BlueKeep-Style Bugs Renew the Risk of a Windows Worm, Wired, 8/13/2019, https://www.wired.com/story/dejablue-windows-bugs-worm-rdp/
- Stockley, Mark, RDP exposed: the wolves already at your door, Sophos Naked security, 7/17/2019, https://nakedsecurity.sophos.com/2019/07/17/rdp-exposed-the-wolves-already-at-your-door/
- Carroll, Eoin; Mundo, Alexandre; Laulheret, Philippe; Beek, Christiaan; and Povolny, Steve; RDP Stands for “Really DO Patch!” – Understanding the Wormable RDP Vulnerability CVE-2019-0708, McAfee Blogs, 5/21/2019, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/
- Goodin, Dan, Exploit for wormable BlueKeep Windows bug released into the wild, ARS Technica, 9/6/2019, https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/
- Cimpanu, Catalin, Even the NSA is urging Windows users to patch BlueKeep (CVE-2019-0708), ZDNet, 7/4/2019, https://www.zdnet.com/article/even-the-nsa-is-urging-windows-users-to-patch-bluekeep-cve-2019-0708/
- Sophos Community Knowledge Base, CVE-2019-0708: Remote Desktop Services remote code execution vulnerability (known as BlueKeep), 5/29/2019, https://community.sophos.com/kb/en-us/134100
- Microsoft TechNet, Remote Desktop Services (RDS) Component Architecture Poster Windows Server 2008 R2, https://blogs.technet.microsoft.com/danstolts/2010/10/remote-desktop-services-rds-component-architecture-poster-windows-server-2008-r2/

References (continued)

- Foley, Mary Jo, Microsoft patches Windows XP, Server 2003 to try to head off 'wormable' flaw, ZDNet, 5/14/2019, https://www.zdnet.com/article/microsoft-patches-windows-xp-server-2003-to-try-to-head-off-wormable-flaw/
- Cimpanu, Catalin, US company selling weaponized BlueKeep exploit, ZDNet, 7/25/2019, https://www.zdnet.com/article/us-company-selling-weaponized-bluekeep-exploit/
- Microsoft works with researchers to detect and protect against new RDP exploits, Microsoft Security Blog, 11/2/2019, https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/
- Cimpanu, Catalin, Millions of RDP Endpoints Exposed Online and Ready for Bad Things, ZDNet, 8/15/2017, https://www.bleepingcomputer.com/news/security/millions-of-rdp-endpoints-exposed-online-and-ready-for-bad-things/
- Boddy, Matt, Jones, Ben, and Stockley, Mark, RDP Exposed - The Threat That's Already at Your Door, Sophos, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf
- Hudak, Tyler, Adventures of an RDP Honeypot – Part One: RDP Security, TrustedSec Blog, https://www.trustedsec.com/blog/adventures-of-an-rdp-honeypot-part-one-rdp-security/
- Schwartz, Mathew J., Ransomware Gangs' Not-So-Secret Attack Vector: RDP Exploits, Bank InfoSecurity, 11/4/2019, https://www.bankinfosecurity.com/ransomware-gangs-not-so-secret-attack-vector-rdp-exploits-a-13342
- Cimpanu, Catalin, Botnet Fodder: 10 Million Devices With Open Telnet Ports Still Available Online, ZDNet, 7/15/2017, https://www.bleepingcomputer.com/news/security/botnet-fodder-10-million-devices-with-open-telnet-ports-still-available-online/
- McKeague, Brendan, Ta, Van, Fedore, Ben, Ackerman, Geoff, Pennino, Alex, Thompson, Andrew, Bienstock, Douglas, Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware, FireEye, 4/5/2019, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
- Constantin, Lucian, More critical Remote Desktop flaws expose Windows systems to hacking, CSO Online, 8/14/2019, https://www.csoonline.com/article/3431665/more-critical-remote-desktop-flaws-expose-windows-systems-to-hacking.html
- Cimpanu, Catalin, FBI warns companies about hackers increasingly abusing RDP connections, ZDNet, 9/27/2018, https://www.zdnet.com/article/fbi-warns-companies-about-hackers-increasingly-abusing-rdp-connections/
- Stockley, Mark, RDP BlueKeep exploit shows why you really, really need to patch, Sophos Naked security, 7/1/2019, https://nakedsecurity.sophos.com/2019/07/01/rdp-bluekeep-exploit-shows-why-you-really-really-need-to-patch/
- Stockley, Mark, RDP BlueKeep exploit shows why you really, really need to patch, Sophos Naked Security, 7/1/2019, https://nakedsecurity.sophos.com/2019/07/01/rdp-bluekeep-exploit-shows-why-you-really-really-need-to-patch/

References (continued)

- Remote Desktop Protocol, Microsoft Docs, 5/30/018, https://docs.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol?redirectedfrom=MSDN
- CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability, Microsoft Security Update Guide, 5/14/2019, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- CVE-2019-0708, MITRE Common Vulnerabilities and Exposures, 11/26//2018, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
- CVE-2019-0708, CVE Details, 5/16/2019, https://www.cvedetails.com/cve/CVE-2019-0708/
- Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability, Microsoft Windows Security Support, 5/14/2019, https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
- Godin, Dan, Microsoft practically begs Windows users to fix wormable BlueKeep flaw, ARS Technica, 5/31/2019, https://arstechnica.com/information-technology/2019/05/microsoft-says-its-confident-an-exploit-exists-for-wormable-bluekeep-flaw/
- Warren, Tom, Microsoft warns of major WannaCry-like Windows security exploit, releases XP patches, The Verge, 5/14/2019, https://www.theverge.com/2019/5/14/18623565/microsoft-windows-xp-remote-desktop-services-worm-security-patches

Questions

Upcoming Briefs

- Bluekeep
- Incident Response

Image courtesy of Naked Security

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**