



Poisoned RDP

He Said, She Said – Poisoned RDP Offense and Defense





Who Are We?

Dana Baril

Security Researcher

Microsoft Defender ATP

H

🍠 <u>@dana_baril</u>

Eyal Itkin

Security Researcher

Check Point Research CP<



BlueKeep?



- A **different** vulnerability in the Remote Desktop Protocol
 - Unauthenticated RCE in Microsoft's RDP Servers
 - Disclosed by the UK national CERT in May 2019

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability Security Vulnerability

Published: 05/14/2019

• We are going to focus on a **different** attack vector

Motivation

- Lazy Lateral Movement
- "Ambush" privileged users
- IT Staff
 - o Gain credentials
- Malware Researchers
 - Escape isolated virtual machines

Remote Desktop Protocol (RDP)

"Client" "Server"

- Connects to a remote Windows Machine
 - Remote corporate PC / Server
 - o Local / Remote Virtual Machine
- A.K.A. mstsc
- Attack doesn't require "Admin"



Poisoned RDP?



Attack & Take over the victim's computer

RDP Clients



Remote Desktop Connection

×



Do you trust this remote connection?

This remote connection could harm your local or remote computer. Make sure that you trust the remote computer before you connect.



Type: Remote computer: Remote Desktop Connection



🕤 Show Details



Cancel

Our Targets

612

3,210

\star Star

★ Star

68

326

• Open Source RDP Clients

O Watch ▼

O Watch ▼

- o rdesktop
- FreeRDP
- Microsoft's default client
 - \circ mstsc.exe

v	Fork	170				
•	TOTA					
	¥ Fork	1,293				
	💷 Run				:	×
		Type the na resource, an	me of a progran Id Windows wil	n, folder, docun I open it for you.	nent, or Internet	
	<u>O</u> pen:	mstsc			~	
			ОК	Cancel	<u>B</u> rowse	

1. Start with the easiest target

- Pick the simplest open source rdesktop
- Audit the code and learn how RDP works
- Find potentially vulnerable features / modules
- Gradually gain confidence
- Move on when scanned all of the code

Lessons on RDP

- Protocol consists of logical channels
 - BlueKeep exploits the internal (non-public) MS_T120 channel
- Contains multiple authentication methods
- Screen updates are sent using Bitmaps
- Basic Clipboard types are shared

2. Break rdesktop

- Naïve C code with less than minimal checks
 - Almost no checks that minimal input was received
- Found 11 critical vulnerabilities (19 Overall)
- CVEs:
 - CVE 2018-8791 CVE 2018-8800
 - CVE 2018-20174 CVE 2018-20182

3. Find complicated features

• CVE 2018-8795: Integer-Overflow in Bitmap Parsing

16 bits: in uint16 le(s, width) **0x8000** 16 bits: 0x8001 in uint16 le(s, height) 16 bits: 4 in uint16 le(s, bpp) > 32 bits: 0x20000 // Allocate space bmpdata = xmalloc(width * height * bpp) bitmap decompress(bmpdata, width, height, bpp);

4. Break FreeRDP

- The C code looks better
 - Still has a few cracks if we look deep enough
 - Again, vulnerable to Bitmap parsing
- Found 5 critical vulnerabilities (6 Overall)
- CVEs:
 - CVE 2018-8784 CVE 2018-8789

mstsc.exe

🗁 Run



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:	mstsc		•	
			Canad	Descusa
		UK	Cancel	Browse

5. Break mstsc.exe?

- PoCs from previous targets failed 😕
- The code is robust

• Smart buffers check for parsing errors

- Includes many more features
- Where should we go now?

Back to the Doord

- Until now, the clipboard shared text:
 - \circ CF_TEXT
 - CF_UNICODETEXT
- It seems like Microsoft supports many more formats now
- Let's dig into the clipboard

Clipboard 101

- A kernel data structure that stores data
 - One clipboard per session ("connection")
 - Shared between processes
- Stores data (blobs) by ID / Name
- Caution: Clipboard data is not trusted. Parse the data carefully before using it in your application.

👗 InsideClipboa	_	- 🗆	I X				
File Edit View	Options Help						
Format ID 🧳	Format Name	Size	2		^		
◎ 1	CF_TEXT	20					
◎ 7	CF_OEMTEXT	20			v		
This is a text line							
					Y		
<				>			
4 item(s), 1 Selected NirSoft Freeware							

Clipboard 101

- A kernel data structure that stores data
 - One clipboard per session ("connection")
 - Shared between processes
- Stores data (blobs) by ID / Name
- "**Caution:** Clipboard data is not trusted. Parse the data carefully before using it in your application." (MSDN)

🖏 InsideClipboa	_	-	ı x			
File Edit View	Options Help					
🔲 🖸 🖻 😭	ال ال					
Format ID 🧳	Format Name	Size	2		^	
◎ 1	CF_TEXT	20				
◎ 7	CF_OEMTEXT	20			¥	
This is a text line						
					\lor	
<				>		
4 item(s), 1 Selecter	NirSoft F	reeware				

Clipboard Over RDP

- Everything in the clipboard is synchronized automatically
- Black Lists instead of White Lists

Some formats are discarded by ID

• Some formats are discarded by Name



 To avoid syncing "heavy" content, all content is subject to "delayed rendering"

Drag & Drop

- Internally, copying files is called "Drag & Drop"
- Copying files uses multiple formats
 - CF_HDROP lists the file names
 - FileGroupDescriptorW full metadata
 - Many more...
- Let's see how it works in practice













FileGroupDescriptorW

- Proprietary blob structure
- Contains a list of file records
 - Meta data (timestamps)
 - File path filename
- Client passes it directly to the clipboard

Path Canonicalization

@GullOmer: "try to find where they sanitize the path"





Path Traversal Over RDP

- We received a CVE from Microsoft: CVE 2019-0887
- When using "Copy & Paste" a malicious server can:

• Drop arbitrary files to arbitrary locations

• Drop your script in the Startup folder and that's it

Taking it one step further

- The clipboards are **fully** synchronized
 - Ctrl+C updates the clipboard
 - Each update sends a CLIPRDR_FORMAT_LIST
 - The receiver updates his clipboard accordingly
- What does it mean?

Scenario #1 - Eavesdropping

- When the client copies a password we get it too
- This is a **feature** of the synced clipboard
- We know in advance when the client is going to copy a file on his computer

Scenario #2 – Ctrl+V Only Attack

- Once again, ambush the client
- When he copies a file, start the attack
- Send an update message and switch his clipboard to a malicious FGDw
- His Ctrl+V will trigger the path traversal

Did we break them all?



Hyper-V

- Never used it till now
- Installed a Hyper-V machine, and

1	Connect to	o RDP PoC	×	
٦	Display Loc	cal Resources		
	Remote au	idio	_	
		Configure remote audio settings.		
		Settings		
	Local devi	ces and resources		
		Choose the devices and resources that you want to use in your remote session.		
	_	Printers Clipboard		
		More		

Hyper-V? RDP!

- Microsoft uses RDP for accessing virtualized machines
- The GUI connection to the VM is transferred over RDP!
- Our PoC worked on the first attempt
- We just found a Guest-to-Host VM Escape 😊

Hyper-V Demo

https://youtu.be/nSGlMJqQEh0

Note on WDAG and friends

- Windows Defender Application Guard
 - Browsing "risky" sites with a virtualized Edge browser
- Uses hvsirdpclient.exe instead of mstsc.exe
- This time, MS uses White-lists instead of Black-Lists
 - o Clipboard is off by default
 - The clipboard permits only 2 format types: Text & Images
- The White list blocks our vulnerability, good job ☺

Defense

VULNERABILITY DETECTED

PATCH EVERYTHING NOW!

imgflip.com

A patch is not enough

- Users remain vulnerable until they install patch
- Detect using existing telemetry
- Detection must be implemented on "victim" machine
- RDP anomaly detection won't cut it

Event Tracing for Windows (ETW)

• Kernel-level tracing facility that lets you log kernel or application-defined events

🛃 Event Viewer		
File Action View Help		
🗢 🤿 🙍 📰 🚺 🖬		
🛃 Event Viewer (Local)	Security Number of events: 603	Actions
> 📑 Custom Views	Keywor Date and Time Source Event ID Task C	Security 🔺
Application	Audi 7/11/2019 3:11:03 PM Micros 5379 User A	Open Saved Log
Security	Q Audi 7/11/2019 3:11:03 PM Micros 5381 User A	Create Custom View
Setup	Q Audi 7/11/2019 3:11:01 PM Micros 5381 User A	Import Custom View
🛃 System	Q Audi 7/11/2019 3:10:31 PM Micros 4799 Securit	
Forwarded Events	Audi 7/11/2019 3:10:31 PM Micros 4799 Securit	Clear Log
Applications and Services Lo	Audi 7/11/2019 3:10:24 PM Micros 4672 Special	Filter Current Log
up subscriptions		Properties
	Event 53/9, Microsoft Windows security auditing.	🙀 Find
	General Details	Save All Events As
		Attach a Task To this L.,
	Credential Manager credentials were read.	View
	Subject:	
	Security ID: DESKTOP-T50GBF5\Demo	Q Retresh
	Account Name: Demo Account Domain: DESKTOP-T50GBF5	I Help
	Logon ID: 0x2A1D86	Event 5379, Microsoft Wind 🔺
	Read Operation: Enumerate Credentials	Event Properties
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.	Attack Tack To This Ev
		Copy
	Log Name: Security	Save Selected Events
	Source: Microsoft Windows security Logged: 7/11/2019 3:11:03 PM	Refresh
	Event ID: 53/9 Task Category: User Account Management	Help +
	Level: Information Keywords: Audit Success	
	User: N/A Computer: DESKTOP-150GBF5	
	More information: Event Log Unline Help	

RDP Connections Events

Provider Guid: 1139c61b-b549-4251-8ed3-27250a1edec8

Microsoft-Windows-RemoteDesktopServices-RdpCoreTS

Event 131, RemoteDes	ktopServices-RdpCoreTS				Event 132, RemoteDe	sktopServices-RdpCoreTS			
General Details					General Details				
The server accepte	ed a new UDP connection from	client [172.17.1	91.113]:57022.		A channel rdpgrfx	has been connected between	the server and th	e client using transport tunnel:	0.
Log Name:	Microsoft-Windows-Remotel	DesktopServices	-RdpCoreTS/Operational		Log Name:	Microsoft-Windows-Remote	DesktopServices-	RdpCoreTS/Operational	
Source:	RemoteDesktopServices-Rdg	Logged:	7/11/2019 3:24:18 PM		Source:	RemoteDesktopServices-Rdp	Logged:	7/11/2019 3:24:18 PM	
Event ID:	131	Task Category:	RemoteFX module	ſ	Event ID:	132	Task Category:	RemoteFX module	
Level:	Information	Keywords:			Level:	Information	Keywords:		
User:	NETWORK SERVICE	Computer:	DESKTOP-T5OGBF5		User:	NETWORK SERVICE	Computer:	DESKTOP-T5OGBF5	
OpCode:	EstablishConnection				OpCode:	EstablishConnection			
More Information:	Event Log Online Help				More Information:	Event Log Online Help			

Events 131 – accepting connection

Event 132 – channel connected

Clipboard Events

Non-manifested provider, tracing clipboard API usages

Provider guid: 3e0e3a92-b00b-4456-9dee-f40aba77f00e

Microsoft.Windows.OLE.Clipboard

Task name: OLE_Clipboard_MethodDiagnostics

Message/PartC

ApiName: CClipDataObject::GetData CLIPFORMAT: Performed DropEffect ClipboardDataObjectTask: 0x0 HRESULT: 0x80040064 MatchFormatetc: 1 STGMEDIUM: 0x9BDA00 m_pDataObject: 0x6404478 tymed: 1

Clipboard Events

- Selected properties:
 - ApiName: GetData, SetData
 - CLIPFORMAT: Returned clipboard format (bitmap, text, Unicode text, etc.).
 - HRESULT: Api HResult
 - Tymed: Paste destination medium
- No clipboard content!



Telemetry Demo

https://www.youtube.com/watch?v=q9Lox_rfqvw

Detection Logic – Basic

• While in RDP:

1. When multiple files are copied in a short period of time

2. Triggers a scan

File Creation Events

- In order to overcome the file information gap, we need more data!
- Security products have file creation indications

Detection Logic

- While in RDP:
 - 1. When multiple files are copied in a short period of time
 - 2. Correlate file creation with the same timestamps
 - 3. If the correlated files are in different directories alert!

More Detection Logics

- Startup folder as a destination
 - Anomaly detection
 - Files scanning
- Clipboard as an attack vector
 - File pasting anomaly number of pasted files or the files directories
- Malicious files dropping
 - File creation anomaly file path, creation time and file name

OS Patch

• Verify the RDP clipboard: ValidateFilePaths

000000016AB893FC	CFormatData	Packer::DecodeFormatData(void * *,ulong,uchar *,ulong)				
000000016AB89640	call	?FileDescriptorW@CClipFormatTypes@@QEAAIXZ				
000000016AB89645	xor	b4 r9d , b4 r9d				
000000016AB89648	mov	b4 r8d, b4 ebp	11	unsigned	int	
000000016AB8964B	cmp	b4 ebx, b4 eax				
000000016AB8964D	mov	rdx, r14	11	unsigned	int8	*
000000016AB89650	lea	rax, ss:[rsp+arg_10]				
000000016AB89655	setz	b1 r9b	11	int		
000000016AB89659	mov	ss:[rsp+var_28], rax	11	int *		
000000016AB8965E	call	?ValidateFilePaths@CFormatDataPacker@@AEAAJPEAEKHPEAH@Z				
000000016AB89663	mov	b4 ebx, b4 eax				
000000016AB89665	test	b4 eax, b4 eax				
000000016AB89667	jns	0x16AB896AD				

• Verify canonical path before pasting:

pszFilename = pCurrentFileRecord->szFilename; status_code = PathCchCanonicalize(&pszPathOut, 0x104ui64, pszFilename); if ((status_code & 0x8000000) != 0) {

What have we learned ?

- Design lesson: Think twice before connecting different modules
 - \circ . Clipboards were designed to be used locally, and therefore trusted
 - When sharing across machines it made sense to enable clipboard sharing
 - However, this exposed machines to clipboards they can no longer trust
- Windows telemetry is an important tool in the defender's toolbox
- Our industry can benefit from cross-community collaborations

That's all folks

Remote Desktop Connection



Your Remote Desktop session has ended, possibly for one of the following reasons:

The administrator has ended the session. An error occurred while the connection was being established. A network problem occurred.

For help solving the problem, see "Remote Desktop" in Help and Support.

OK

Help

@dana_baril

