A Decade After Stuxnet’s Printer Vulnerability

**Printing is still the Stairway to Heaven**

Peleg Hadar  Senior Security Researcher &  Tomer Bar  Research Team Lead

SafeBreach LABS
Peleg Hadar  Senior Security Researcher

- 7+ years in InfoSec
- Senior Security Researcher @ SafeBreach Labs
- Main focus in Windows internals and vulnerability research
- @peleghd
Tomer Bar  
Research Team Lead

- 15+ years in Cyber Security
- Research Team Lead @ SafeBreach Labs
- Main focus in APT and vulnerability research
- Past publications:
  - Prince of Persia - Terminating 10 Years Campaign For Fun And Profit
  - Infy Malware Active In Decade Of Targeted Attacks
  - KasperAgent and Micropsia - Targeted Attacks In The Middle East
  - Ride The Lightning With Foudre
  - Double Edge Sword Attack - Exploiting Quasar Rat Command and Control
  - BadPatch (APT-C-23)
Agenda Is Stuxnet 2.0 possible?

- Analysis of Stuxnet’s propagation capabilities (vulnerabilities)
  - Root Cause
  - Patch
  - Re-Exploitation / Equivalent newer vulnerability in the same component

- Our Research
  - How did we re-exploited a patched 10 years old MS Windows vulnerability
  - Demonstration of 2 unpatched 0-day vulnerabilities (Pre-coordinated with Microsoft)

- Mitigations and Suggestions
  - Better Patch
  - Better real-time prevention for an entire bug class
Agenda two main takeaways

Stuxnet 2.0
Is it possible to re-occur?

Patch effectiveness
Is it possible to abuse patched vulnerabilities?
Terminology

Narrow Patch

Patch
According to JOHN BUMGARNER, CTO @ U.S. CYBER CONSEQUENCES UNIT
Stuxnet As Seen in “0 Days”
**Stuxnet Main Building Blocks**

**Propagation Capabilities**
- 5 Vulnerabilities
- 3 RCE
- 2 LPE

**Evasion Capabilities**
- Rootkit
- Stolen Certificate

**ICS Capabilities**
- ICS Target Detection
- Siemens Related Actions
- Final Payload
“Now, over 22 million pieces of malware use that blueprint to attack organizations and states...” -regdox.com
Spooler Propagation Capabilities

- MS10-046 (LNK)
- MS06-040 (RPC)
- MS10-092 (Task Scheduler)
- MS10-073 (Win32k)
- MS10-061 (Spooler)
LNK Stuxnet’s 0-day - Root Cause

LNK File

Pointer to an Icon Resource

LoadLibrary

CPL (DLL) File

Icon Resource
Malicious Code
LNK 0-Day Exploitation Paths Overview

CVE-2010-2568

LoadAndFindApplet

CPL_LoadCPLModule

Payload Execution Function

LoadLibraryW
The patch did not modify this call!

LoadLibraryW

IsRegisteredCPL && StrToIntW(wszIconId) == 0

NO

User-controlled input from LNK

CPL_LoadCPLModule

Payload Execution Function

Don’t Load CPL, Change IconID to -1

YES
LNK 0-Day Exploitation Paths Overview

CWE-2010-2568

LoadAndFindApplet

IsRegisteredCPL && StrToIntW(wszIconId) == 0

YES

Don’t Load CPL, Change IconID to -1

CWE-2015-0096

User-controlled input from LNK

NO

CPL_LoadCPLModule

Payload Execution Function

The patch did not modify this call!

LoadLibraryW

Narrow Patch

The patch did not modify this call!
Truncated to 260 Wide Chars
\[c:\Ma.dll,-1,AA...AAA\]

554 Wide Chars
\[c:\Ma.dll,-0\]

\[int\ \text{dwIconId} = \text{StrToIntW}(L"-"\)\]
\[\text{dwIconId will be 0}\]
LNK 0-Day Exploitation Paths Overview

- **CVE-2010-2568**
  - Narrow Patch

- **CVE-2015-0096**
  - Narrow Patch

- **LoadAndFindApplet**

- **IsRegisteredCPL**
  - NO
    - **CPL_LoadCPLModule**
      - Payload Execution Function
        - The patch did not modify this call!
      - **LoadLibraryW**
        - The patch did not modify this call!

- **MS015-020**
  - Buffer truncation issue was fixed
  - StrToIntW removed

- **Narrow Patch**

- **Don’t Load CPL**
0-Day Exploitation Paths Overview

CVE-2010-2568
- Narrow Patch
  - LoadAndFindApplet

CVE-2015-0096
- Narrow Patch
  - CPL_LoadCPLModule
    - Payload Execution Function
      - LoadLibraryW

CVE-2017-8464
- _DecodeSpecialFolder
  - _GetPidlFromAppletId
LNK 0-Day Exploitation Paths Overview

CVE-2010-2568
CVE-2015-0096
CVE-2017-8464

LoadAndFindApplet
_GetPidlFromAppletId
_LoadCPLModule
_LoadLibraryW

CVE-2017-8464 - Patch
- Added previous validation to validate if CPL is registered

Narrow Patch
Narrow Patch

Payload Execution Function
LNK 0-Day Exploitation Paths Overview

- **CVE-2010-2568**
  - Narrow Patch
  - **LoadAndFindApplet**

- **CVE-2015-0096**
  - Narrow Patch

- **CVE-2017-8464**
  - **_DecodeSpecialFolder**
  - **_GetPidlFromAppletId**
  - **_NextNonCachedCpl**

- **Not been exploited yet**

**Payload Execution Function**

**CPL_LoadCPLModule**

**LoadLibraryW**

The patch did not modify this call either!
**Spooler**  Printing our Way to SYSTEM

- MS10-046 (LNK)
- MS06-040 (RPC)
- MS10-092 (Task Scheduler)
- MS10-073 (Win32k)
- MS10-061 (Spooler)

- CVE-2015-0096 (LNK)
- CVE-2017-8464 (LNK)
RPC

2006

MSRC - 1st Vulnerability - **Limited Scope**
“Very limited, targeted attacks”

"As a reminder, Microsoft is aware of very limited, targeted attacks that exploited the vulnerability prior to the release of the update, but we’re not currently seeing broad attacks that use this newly posted exploit code"

~Microsoft Security Response Center

2009

**Wide spread** - The same vulnerable dll was exploited By Stuxnet & Conficker Worm

Conficker HeatMap

RPC Path Canonical path

Path Canonization

absolute path: canonical path:
C:\xxx\..\abc\file.txt  ---->  C:\abc\file.txt

It allows textual comparison of two different representation of the same canonical path

C:\xxx\..\abc\xxx\..\file.txt  ==  C:\xxx\..\abc\file.txt  == C:\abc\file.txt
The vulnerable function allocates 0x414 bytes of space, **but** limits the length of the Path to 0x411 **Unicode** chars (0x822 bytes).

```
dce=Pex::DCERPC->new(...)
$dce->request(handle, 0x1f, stub(including path )
```
RPC - Exploitation Paths Overview

CVE-2006-3439

NetpWPathCanonicalize

Stack OOB write Primitive

WcsCat
MS06-040 Patch

1. Check if path length is more than 0x207
2. Omit the \texttt{wcscat} function call
RPC Exploitation Paths Overview

https://dontstuffbeansupyourownose.com/2008/10/23/looking-at-ms08-067/
RPC The Patch - MS08-067

CVE-2006-3439
CVE-2008-4250

NetpRPathCanonicalize
NetpWPathCanonicalize

_Wcscat
Stack OOB write Primitive

_Wcscpy
Stack OOB write Primitive

_StringCopyWorkerW
Task Scheduler LPE - CVE-2010-3338 - Root Cause

The Patch - MS10-092
Microsoft has implemented a 2nd integrity check SHA-256 using ComputeHash function.

A registered job

```xml
<Principals>
  <Principal id="LocalSystem">
    <UserId>S-1-5-18</UserId>
    <RunLevel>HighestAvailable</RunLevel>
  </Principal>
</Principals>
<Actions Context="LocalSystem">
  <Exec>
    <Command>C:\WINDOWS\NOTEPAD.EXE</Command>
    <Arguments></Arguments>
  </Exec>
</Actions>
```

A crafted job with a forged CRC32

```xml
- <Principals>
  - <Principal id="LocalSystem">
    <UserId>S-1-5-18</UserId>
    <RunLevel>HighestAvailable</RunLevel>
  </Principal>
</Principals>
- <Actions Context="LocalSystem">
  - <Exec>
    <Command>C:\WINDOWS\NOTEPAD.EXE</Command>
    <Arguments />
  </Exec>
</Actions>
```

- Added bytes will change back the CRC32 value to bypass the integrity check
- The xml command is modified to execute the malicious code

Source: https://aroundcyber.files.wordpress.com/2012/11/stuxnet_under_the_microscope.pdf
Task Scheduler LPE - CVE-2019-1069

CVE-2019-1069 - new Task Scheduler LPE

Task Scheduler stores tasks as files in two separate locations:
C:\Windows\Tasks < ----(legacy location).
C:\Windows\System32\Tasks

Sending an RPC request to the service for modifying a legacy-located task will migrate it to the preferred location of C:\Windows\System32\Tasks.

Task Scheduler CVE-2019-1069 - Patch

_CschRpcSetSecurity

SetJobFileSecurityByName

CreateFile

VerifyJobFilePath

GetFinalPathNameByHandleW

GetFinalPathNameByHandleW

nNumberOfLinks <= 1

&& OriginalPath == FinalPath

ELSE

ACCESS DENIED

SetSecurityInfo

CVE-2019-1069
<table>
<thead>
<tr>
<th>CVE-2020-0720</th>
<th>Win32k Elevation of Privilege Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-0721</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0722</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0723</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0725</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0726</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0731</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
<tr>
<td>CVE-2020-0719</td>
<td>Win32k Elevation of Privilege Vulnerability</td>
</tr>
</tbody>
</table>
Spooler Propagation Capabilities

MS10-046 (LNK)
- CVE-2015-0096 (LNK)
- CVE-2017-8464 (LNK)

MS06-040 (RPC)
- MS08-067 (RPC)

MS10-092 (Task Scheduler)
- CVE-2019-1069 (Task Scheduler)

MS10-073 (Win32k)
- CVE-2020-0720 (Win32k)
- CVE-2020-0721 (Win32k)

MS10-061 (Spooler)
Our Research
20+ Year-old Bug in 20 Minutes of Fuzzing
Spooler SHD and SPL files

Printing Jobs

\Windows\System32\spool\PRINTERS

00001.SPL
Data to Print

00001.SHD
Metadata of print job

Writable folder by all users

SHD is processed once service is started

ProcessShadowJobs( NULL, pIniSpooler );
After 20 minutes...

```c
ntdll!RtlLengthSecurityDescriptor+0x60: 00007fff 881cbe70 0fb64001 movzx eax,byte ptr [rax+1] ds:8c040001`00000001=??
Resetting default scope

EXCEPTION_RECORD: (.exr -1)
ExceptionAddress: 00007fff881cbe70 (ntdll!RtlLengthSecurityDescriptor+0x0000000000000060)
ExceptionCode: c0000005 (Access violation)
ExceptionFlags: 00000000
NumberParameters: 2
  Parameter[0]: 0000000000000000
  Parameter[1]: ffffffff00000000
Attempt to read from address ffffffff00000000
```
Spooler Crash Demo
Print Spooler (Printing to a File)
Print Spooler (Printing to a File)
Spooler 0-Day Exploitation Paths Overview

- CVE-2010-2729
- CreateFileW
- StartDocPrinterW
- PrintingDirectlyToPort
- LcmStartDocPort
- RPC
  - Narrow Patch
Spooler MS10-061 Patch Bypass #1

- **CVE-2020-1048**
  - StartDocPrinterW
  - Narrow Patch
- **CVE-2010-2729**
  - ValidateOutputFile
  - CheckLocalCall

**YES**
- PrintingDirectlyToPort
- **ACCESS DENIED**

**NO**
- LcmStartDocPort
- CreateFileW
Spooler Arbitrary Printer Port Creation

PS C:\Users\Johnny> Add-PrinterPort c:\windows\system32\wbem\wbemcomn.dll
PS C:\Users\Johnny> Add-Printer "MS Publisher Color Printer" -DriverName -PortName "c:\windows\system32\wbem\wbemcomn.dll"
Spooler  The Impersonation Barrier

Operation: CreateFile
Result: ACCESS DENIED
Path: C:\Windows\System32\wbem\wbemcomn.dll
Duration: 0.0002281

Desired Access: Generic Write, Read Attributes
Disposition: OpenIf
Options: Sequential Access, Synchronous
Attributes: N
AllocationSize: 0
Impersonating: P-MVM\p

Accessing the file using the access token of the client
Spooler CVE-2020-1048 Root Cause

Limited User → Print Spooler Initialization → 00001.SHD Print Port Path

ProcessShadowJobs → Print Pre-Written Jobs (Saved as SHD files)

SYSTEM Token

Print Port Path

C:\Windows\System32\Wbem\Wbemcommn.dll

Operation: CreateFile
Result: REPARSE
Path: C:\Windows\System32\Wbem\Wbemcommn.dll
Duration: 0.0000160

Desired Access: Generic Write, Read Attributes
Disposition: OpenIf
Options: Sequential Access, Synchronous
Attributes: N
ShareMode: Read
AllocationSize: 0
Impersonating: NT AUTHORITY\SYSTEM
OpenResult: <unknown>
Spooler MS10-061 Patch Bypass #2

```c
hOutputFile = CreateFileW(szOutputFile, GENERIC_WRITE,
  if ( hOutputFile == INVALID_HANDLE_VALUE )
    if ( GetLastErro()'') == ERROR_ACCESS_DENIED )
      DllFreeSplMem(v8);
      return bUserAllowedToWriteToOutputFile;
```
Spooler: Printing our Way to SYSTEM

- CVE-2015-0096 (LNK)
- CVE-2017-8464 (LNK)
- MS10-046 (LNK)
- MS06-040 (RPC)
- MS08-067 (RPC)
- MS10-092 (Task Scheduler)
- CVE-2019-1069 (Task Scheduler)
- MS10-073 (Win32k)
- CVE-2020-0720 (Win32k)
- CVE-2020-0721 (Win32k)
- MS10-061 (Spooler)
- CVE-2020-1048 (Spooler)
- CVE-2020-1337 (Spooler)
Spooler  Printing our Way to SYSTEM
Spooler Printing our Way to SYSTEM

Stuxnet 2.0

POSSIBILE!

Is it possible to re-occur?
This is a 0-day and it will be fixed by Microsoft.

Stay tuned for our exploit blog post which will be released in the next few days (once the vulnerability is fixed).
Mitigations
Recommended Mitigations

Patch effectiveness

Is it possible to abuse patched vulnerabilities?
Recommended Mitigations

- Spooler
- OS Patching
- Real Time Detection & Prevention
- Network Security Controls
- Breach and Attack Simulations
- Security Operation Center
- OS Patching
Recommended Mitigations

A limited user can write to the following paths which leads to multiple vulnerabilities

1. System32\spool\PRINTERS - CVE-2020-1048, CVE-2020-1337, Spooler DoS
2. Spool\drivers\color - CVE-2020-1117 (RCE)
3. System32\tasks - CVE-2019-1069
4. C:\ProgramData\Microsoft\Windows\WER\ReportQueue - CVE-2019-0863
5. c:\windows\debug\WIA
6. c:\windows\PLA - 3 sub directories.

C:\>echo "MZmy malicious arbitrary file write" > c:\windows\system32\Safebreach.exe
Access is denied.

C:\>echo "MZmy malicious arbitrary file write" > c:\windows\system32\spool\PRINTERS\Safebreach.exe

C:\>echo "MZmy malicious arbitrary file write" > c:\windows\system32\spool\drivers\color\Safebreach.exe

C:\>echo "MZmy malicious arbitrary file write" > C:\ProgramData\Microsoft\Windows\WER\ReportQueue\Safebreach.exe

C:\>echo "MZmy malicious arbitrary file write" > c:\windows\debug\WIA\Safebreach.exe

C:\>echo "MZmy malicious arbitrary file write" > c:\windows\PLA\reports\Safebreach.exe
The additional vector for CVE-2020-1048 will be addressed in August 2020 as CVE-2020-1337

~Microsoft Security Response Center

The technique results in a local Denial of Service; which doesn't meet Microsoft’s servicing bar for security updates

~Microsoft Security Response Center
Related Work

- **Alex Ionescu & Yarden Shafir** - PrintDemon
- **Dave Weinstein** - Full details on CVE-2015-0096 and the failed MS10-046 Stuxnet fix
- **ITh4cker** - Windows Lnk Vul Analysis: From CVE-2010-2568 to CVE-2017-8464
- **Jeongoh Kyea** - CVE-2020-1770 - Print Spooler EoP Vulnerability
Released Tools

- CVE-2020-1048 - Exploit PoC
- 0-day Spooler ServiceS DoS - Exploit PoC
- Arbitrary File Write Mitigation - Driver
- On August 12th - CVE-2020-1337 - Exploit PoC

https://github.com/SafeBreach-Labs/Spooler
See you next time on - BLACK C(H)AT

Peleg Hadar Senior Security Researcher & Tomer Bar Research Team Leader
Thank You!