

LAB: STATIC ANALYSIS TOOL(CPPCHECK)

NAME: Ishani Bandyopadhyay

ID: 201801102

ANALYSIS TOOL: **cppcheck**

LANGUAGE: C++

GITHUB REPOSITORY: <https://github.com/rajkosto/TegraRcmSmash>

GITHUB CODE: <https://github.com/rajkosto/TegraRcmSmash>

REFERENCE: https://www.youtube.com/watch?v=y_-MT1oXgNM

STEP 1: Installing cppcheck on Windows: <http://cppcheck.sourceforge.net/>

STEP 2: Analyzing the code from the Github Repository with cppcheck.

STEP 3: Checking errors

- Errors
- Warnings
- Style warnings
- Portability warnings
- Performance warnings

Cppcheck 2.4.1 - Project: smasher.cppcheck

File	Severity	Line	Summary	Since date	Tag
TegraRcmSmash-master\Smasher.cpp	portability	406	Assigning an integer to a pointer is not portable.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	61	The address of local variable 'dataBytes' might be accessed at non-zero index.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	61	The address of local variable 'addrData' might be accessed at non-zero index.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	774	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	818	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	868	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 2) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 3) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	1132	%llx in format string (no. 3) requires 'unsigned long long' but the argument type is 'size_t (a...	16-04-2021	

CWE: 758
The address of local variable 'dataBytes' might be accessed at non-zero index.

```
1 #include "Types.h"
2 #include "ScopeGuard.h"
3 #include "WinHandle.h"
4 #include <assert.h>
5 #include <uchar.h>
6 #include <stdio.h>
7 #include <io.h>
8 #include <fcntl.h>
9 #include <iostream>
10 #include <fstream>
11 #include <Shlwapi.h>
12 #include "libusb_k_int.h"
13 #include "iniparse.h"
14
15 class RCHDeviceHacker
16 {
17 public:
18     RCHDeviceHacker(KUSB_DRIVER_API usbDriver, KUSB_HANDLE usbHandle) : usbHandle(usbHandle), usbDriver(usbDriver), totalWritten(0), currentBuffer(0) {}
19     ~RCHDeviceHacker()
20     {
21         if (usbHandle != nullptr)
22         {
23             usbDriver->Free(usbHandle);
24             usbHandle = nullptr;
25         }
26     }
27 }
```

File	Severity	Line	Summary	Since date	Tag
> TegraRcmSmash-master\Smasher.cpp	warning	61	The address of local variable 'dataBytes' might be accessed at non-zero index.	16-04-2021	
> TegraRcmSmash-master\Smasher.cpp	warning	61	The address of local variable 'addrData' might be accessed at non-zero index.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	774	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	818	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	868	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'DWORD (aka un...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 1) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 2) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	warning	886	%u in format string (no. 3) requires 'unsigned int' but the argument type is 'signed int'.	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	portability	1132	%llx in format string (no. 3) requires 'unsigned long long' but the argument type is 'size_t (a...	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	style	1141	Local variable 'copyData' shadows outer variable	16-04-2021	
TegraRcmSmash-master\Smasher.cpp	style	712	Consider using std::find_if algorithm instead of a raw loop.	16-04-2021	

CWE: 686

%u in format string (no. 2) requires 'unsigned int' but the argument type is 'signed int'.

```

874 RCMDeviceHacker rcmDev(Usb, handle); handle = nullptr;
875
876 libusbK::version_t usbKVersion;
877 memset(&usbKVersion, 0, sizeof(usbKVersion));
878 const auto versRetVal = rcmDev.getDriverVersion(usbKVersion);
879 if (versRetVal <= 0)
880 {
881     _ftprintf(stderr, TEXT("Failed to get libusbK driver version for device with win32 error %d\n"), -versRetVal);
882     return -6;
883 }
884 else if (usbKVersion.major != 3 || usbKVersion.minor != 0 || usbKVersion.micro != 7)
885 {
886     _tprintf(TEXT("The opened device isn't using the correct libusbK driver version (expected: %u.%u.%u got: %u.%u.%u)\n"),
887             3, 0, 7, usbKVersion.major, usbKVersion.minor, usbKVersion.micro);
888     _tprintf(TEXT("Please run Zadig and install the libusbK (v3.0.7.0) driver for this device\n"));
889     _ftprintf(stderr, TEXT("Failed to open USB device handle because of wrong driver version installed\n"));
890     return -6;
891 }
892
893
894 u8 didBuf[0x10];
895 memset(didBuf, 0, sizeof(didBuf));
896 const auto didRetVal = rcmDev.readDeviceId(didBuf, sizeof(didBuf));
897 if (didRetVal >= int(sizeof(didBuf)))
898 {
899     _tprintf(TEXT("RCM Device with id %02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X initialized successfully!\n"),
900             didBuf[0], didBuf[1], didBuf[2], didBuf[3], didBuf[4], didBuf[5], didBuf[6], didBuf[7], didBuf[8], didBuf[9], didBuf[10], didBuf[11]);
901 }

```