

PA193 Secure coding principles and practices: Code Review (Part III)
Matus Nemec, Pankaj Agarwal, Anupam Gupta (Team B)

PROJECT (TEAM C): This parser can read ID3 tags but only in version 2.4.

CODE STATISTICS: Code was good, structured, compact and robust.

- Id3v2parser.c (645 lines including comments, description etc.)
- Id3v3parser.h (465 lines including comments , description etc.) + 1 sample.mp3 file 181 KB

1) What Tests were performed?

- a. Automated Tests : CppCheck, Flawfinder, Splint, Clang, zzuf fuzzer
- b. Manual Review: Code Walkthrough
 - i. No checks of return values on file handling as well as UDF functions.
 - ii. Memory allocation and de-allocation (Language tag not freed).
 - iii. Use of hex editor to modify the .mp3 which resulted in skipping those tags.
 - iv. Though deprecated functions are used they are then tried to be handled explicitly in User Defined Functions. Sometimes it throws **false positive**.
 - v. It was revealed that the buffer length checks are not being handled properly.

2) What did you focus upon?

- a. Function Return value checks
- b. Usage of deprecated functions
- c. String format vulnerabilities as code had numerous string functions

3) What did you find out?

- i. CPPCheck: 2 bugs found: Memory Leak, Format String
- ii. Flawfinder: 17 bugs found : Format string , deprecated functions
- iii. Splint : 17 bugs found :Memory Leak, Format String, Return value unchecked, Type Mismatch.
- iv. Clang: 7 bugs found :Format string
- v. Fuzzer (zzuf) : Signal 9(Memory Exceeded) Signal 11 (SIGSEGV)

Extracts (Fuzzer) : With different seed and file ratio the fuzzed file generated.

Line No	String Fn	Cause	Remarks
423	snprintf	Reading beyond the buffer size	Mainly SIGSEGV (signal 11) & Memory Exceeded (signal 9) occurred
398	strncpy		
350	snprintf		
300	snprintf		
455	memcpy		

Extracts (Other Tools)

Bug type	Number of occurrence for this Error type			
	Cppcheck	flawfinder	splint	Clang
Memory leak	1	-	2	-
Format string	1	10	8	7
No check on return value	-	-	6	-
Type mismatch	-	-	1	-
Deprecated function	-	7	-	-

Suggestions: Use of safe functions and strict checking on the buffer length (read/write).