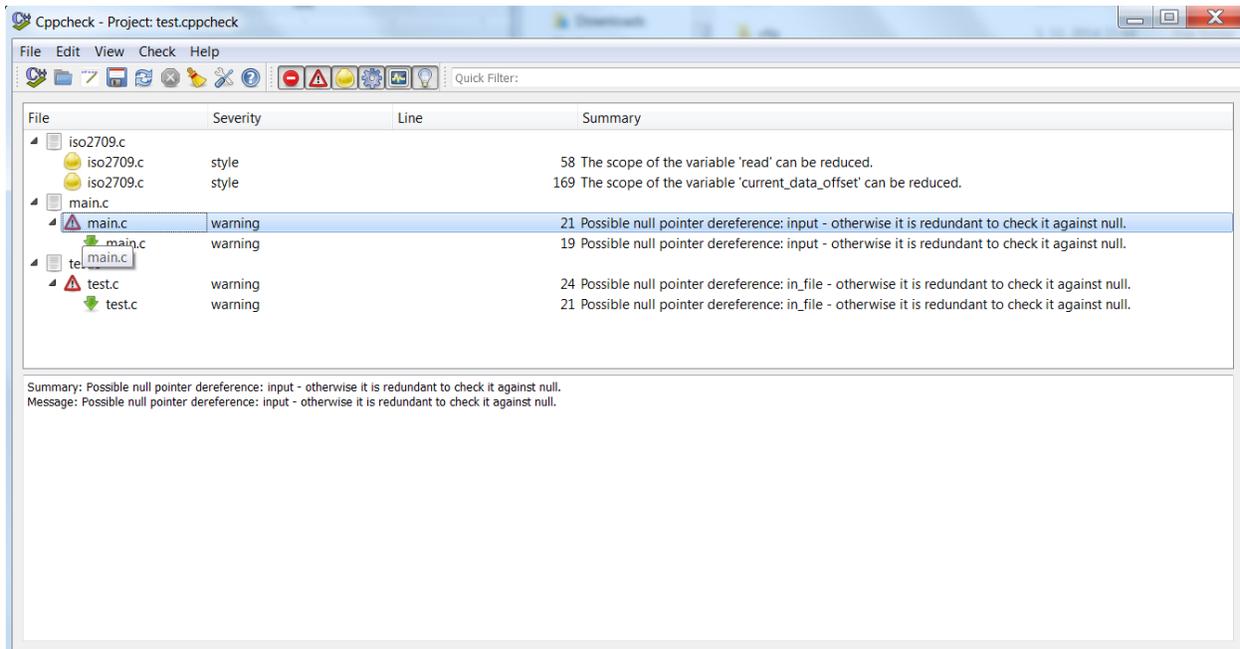


ISO2709 parser code analysis

(Team G)

Platform specific parser (using POSIX regex functions) written in pure C99. ISO format specification is not freely available, but sources contains readme file with nice explanations. Also many input test files are provided (looks Team G tries to do their best).

CPPcheck output:



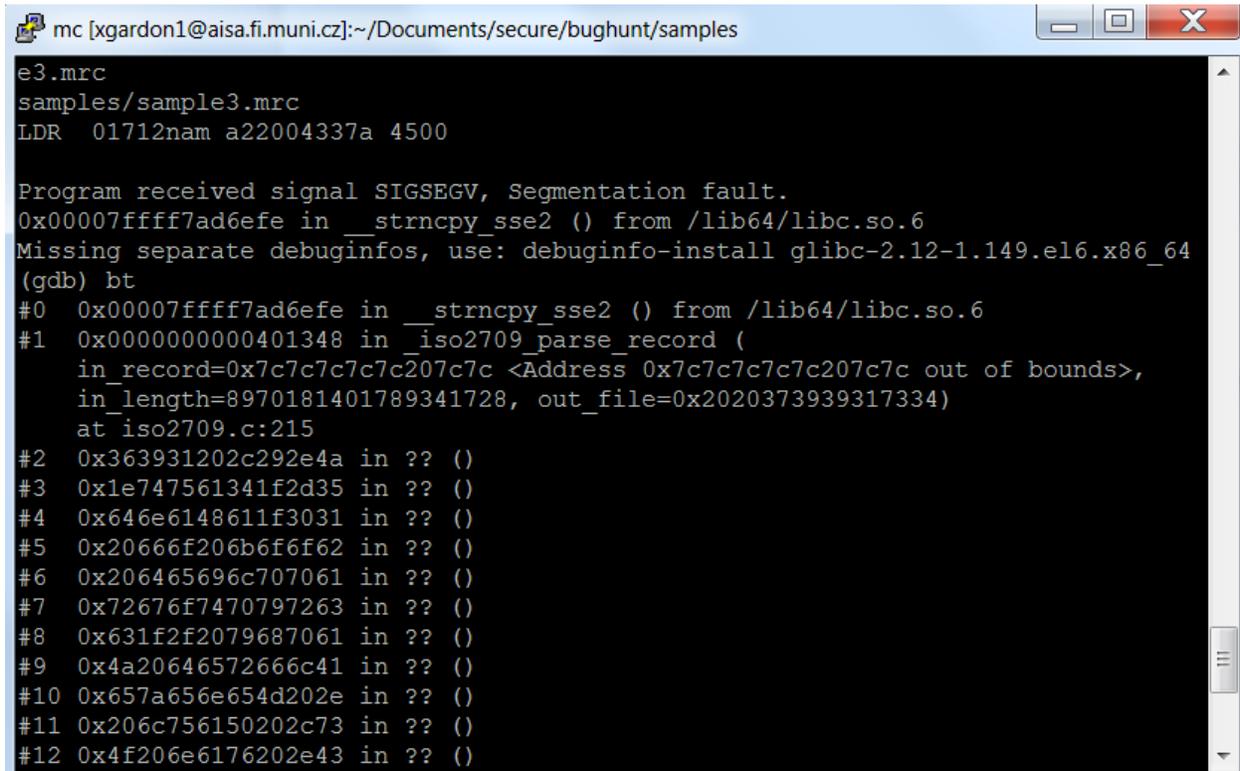
As can be seen in image only 1 warning is shown in main.c file and 2 style information in iso2709.c (parser core) file. In fact found warning can not be used as vulnerability, but leads us to first serious parsers bug.

Found important bugs:

main.c:21	<code>fclose(input);</code>	It tries to close unopened file in error flow (cant read file) == sigsegv
iso2709.c:260	<code>//skip possible white space before record</code>	size of record is hardcoded to "1024 * 100", but if it contains enough whitespace characters parser return error == bug
iso2709.c:260	<code>strncpy(...)</code>	corrupted field definition (strncpy?)

		== sigsegv
--	--	------------

In third case, authors expect 3 numbers (3 bytes, 4 bytes, 5 bytes) in input stream and checks its by regex so only digits are possible values. But if one of digit is changed to special character "0x00" (null byte), regex did not complain. And passed null byte provides SigSegv in strncpy function.



```
mc [xgardon1@aisa.fi.muni.cz]:~/Documents/secure/bughunt/samples
e3.mrc
samples/sample3.mrc
LDR 01712nam a22004337a 4500

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7ad6efe in __strncpy_sse2 () from /lib64/libc.so.6
Missing separate debuginfos, use: debuginfo-install glibc-2.12-1.149.el6.x86_64
(gdb) bt
#0 0x00007ffff7ad6efe in __strncpy_sse2 () from /lib64/libc.so.6
#1 0x000000000401348 in _iso2709_parse_record (
    in_record=0x7c7c7c7c207c7c <Address 0x7c7c7c7c207c7c out of bounds>,
    in_length=8970181401789341728, out_file=0x2020373939317334)
    at iso2709.c:215
#2 0x363931202c292e4a in ?? ()
#3 0x1e747561341f2d35 in ?? ()
#4 0x646e6148611f3031 in ?? ()
#5 0x20666f206b6f6f62 in ?? ()
#6 0x206465696c707061 in ?? ()
#7 0x72676f7470797263 in ?? ()
#8 0x631f2f2079687061 in ?? ()
#9 0x4a206465726666c41 in ?? ()
#10 0x657a656e654d202e in ?? ()
#11 0x206c756150202c73 in ?? ()
#12 0x4f206e6176202e43 in ?? ()
```

Other bugs:

- + Style bugs found by CppCheck
- + In main function, return value is not checked from parser core API (Application end successfully even if error happens)
- + Why all functions check parameters?