

- Secrets
- ABAP
- Apex
- C**
- C++
- CloudFormation
- COBOL
- C#
- CSS
- Flex
- Go
- HTML
- Java
- JavaScript
- Kotlin
- Kubernetes
- Objective C
- PHP
- PL/I
- PL/SQL
- Python
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML



C static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your C code

All rules **311**

Vulnerability **13**

Bug **74**

Security Hotspot **18**

Code Smell **206**

Quick Fix **14**

Tags

Search by name...



"memset" should not be used to delete sensitive data

Vulnerability

POSIX functions should not be called with arguments that trigger buffer overflows

Vulnerability

XML parsers should not be vulnerable to XXE attacks

Vulnerability

Function-like macros should not be invoked without all of their arguments

Bug

The address of an automatic object should not be assigned to another object that may persist after the first object has ceased to exist

Bug

"pthread_mutex_t" should be unlocked in the reverse order they were locked

Bug

"pthread_mutex_t" should be properly initialized and destroyed

Bug

"pthread_mutex_t" should not be consecutively locked or unlocked twice

Bug

Functions with "noreturn" attribute should not return

Bug

"memcpy" should only be called with pointers to trivially copyable types with no padding

Bug

Macros used in preprocessor directives should be defined before use

Analyze your code

Bug Major based-on-misra preprocessor

An attempt to use an undefined identifier may elicit a warning from the preprocessor. Or it may not; the preprocessor may simply assume that the undefined token has a value of 0.

Therefore macro identifiers should not be used in preprocessor directives until after they have been defined, and this limited usage should be enforced with the use of definition tests.

Noncompliant Code Example

```
#if x > 0 /* x assumed to be zero if not defined */
#include SOMETHING_IMPORTANT
#endif

#ifdef y /* Okay; y is not evaluated */
#if y > 0 /* Okay; y must be defined to reach this point */
...
#endif
#endif
```

Compliant Solution

```
#define x 10
...
#if x > 0
#include SOMETHING_IMPORTANT
#endif




#if defined ( y ) && ( y > 0 ) /* more compact form, same result
...
#endif
```

See

- MISRA C:2004, 19.11 - All macro identifiers in preprocessor directives shall be defined before use, except in #ifdef and #ifndef preprocessor directives and the defined() operator.
- MISRA C:2012, 20.9 - All identifiers used in the controlling expression of #if or #elif preprocessing directives shall be #define'd before evaluation

Available In:

sonarlint | sonarcloud | sonarqube Developer Edition

Stack allocated memory and non-owned memory should not be freed  Bug
Closed resources should not be accessed  Bug
Dynamically allocated memory should be released  Bug
Freed memory should not be used