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

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

Objects with integer type should not be converted to objects with pointer type

Analyze your code

Bug | Major | based-on-misra cert

Converting an integer type to a pointer generally leads to unspecified behavior. There are several cases where it might be legitimate:

- Converting the integral literal `0` to the null pointer (but you should use `nullptr` instead, see {rule:cpp:S4962}),
- Converting back to a pointer a pointer value that was converted to a large enough integer (see {rule:cpp:S1767}),
- On embedded devices, device drivers... converting a hard-coded address to a pointer to read some specific memory (this often goes together with the use of `volatile`, since such memory values can change from the outside of the program).

Since even legitimate cases are corner cases that require to be reviewed carefully, this rule simply reports all places where an integer is cast into a pointer (except the literal `0`).

Noncompliant Code Example

```
struct S {
  int i;
  int j;
};

void f(void* a);

void g(int i) {
  S* s1 = (S*)i; // Noncompliant
  f((void*)i); // Noncompliant
}
```

See

- MISRA C++ 2008, 5-2-8 - An object with integer type or pointer to void type shall not be converted to an object with pointer type.
- CERT, INT36-C. - Converting a pointer to integer or integer to pointer

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