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

Freed memory should not be used

Analyze your code

Bug ● Blocker cwe symbolic-execution cert

Once a block of memory has been `freed`, it becomes available for other memory requests. Whether it's re-used immediately, some time later, or not at all is random, and may vary based on load. Because of that randomness, tests may pass when running locally, but the odds are that such code will fail spectacularly in production by returning strange values, executing unexpected code, or causing a program crash.

Noncompliant Code Example

```
char *cp = malloc(sizeof(char)*10);

// ...
free(cp);

cp[9] = 0;  // Noncompliant
```

See

- MITRE, CWE-416 - Use After Free
- CERT, MEM30-C. - Do not access freed memory
- CERT, MEM50-CPP. - Do not access freed memory
- CERT, EXP54-CPP. - Do not access an object outside of its lifetime

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