

-  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



## Objective C static code analysis

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

- All rules** 315
-  Vulnerability 10
-  Bug 75
-  Security Hotspot 18
-  Code Smell 212
-  Quick Fix 13


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

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

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  |
|  Bug                |
| Memory locations should not be released more than once   |
|  Bug                |
| Memory access should be explicitly bounded to prevent buffer overflows                               |
|  Bug                |
| Printf-style format strings should not lead to unexpected behavior at runtime                        |
|  Bug                |
| Recursion should not be infinite   |
|  Bug                |
| Resources should be closed   |
|  Bug              |
| Hard-coded credentials are security-sensitive  |
|  Security Hotspot |
| "goto" should jump to labels declared later in the same function                                     |
|  Code Smell       |
| Only standard forms of the "defined" directive should be used  |
|  Code Smell       |
| Switch labels should not be nested inside non-switch blocks  |
|  Code Smell       |

Loops should not have more than one "break" or "goto" statement

Analyze your code

 Code Smell  Major  based-on-misra confusing

Restricting the number of exits from a loop is done in the interests of good structured programming. One break or goto statement is acceptable in a loop since this allows, for example, for dual-outcome loops or optimal coding.

Noncompliant Code Example

With the default threshold of 1:

```
for (int i = 0; i < 10; i++) {
    if (...) {
        break;           // Compliant
    }
    else if (...) {
        break;           // Non-compliant - second jump from loop
    }
    else {
        ...
    }
}
while (...) {
    if (...) {
        break;           // Compliant
    }
    if (...) {
        break;           // Non-compliant - second jump from loop
    }
}
```

Compliant Solution

```
for (int i = 0; i < 10; i++) {
    if (...) {
        break;           // Compliant
    }
}
while (...) {
    if (...) {
        break;           // Compliant
    }
}
```

See

- MISRA C:2004, 14.6 - For any iteration statement there shall be at most one break statement used for loop termination.
- MISRA C++:2008, 6-6-4 - For any iteration statement there shall be no more than one break or goto statement used for loop termination.
- MISRA C:2012, 15.4 - There should be no more than one break or goto statement used to terminate any iteration statement

Available In:   Developer Edition