rules.sonarsource.com

C static code analysis: "sizeof" should not be called on pointers

2-3 minutes

`sizeof` returns the size in bytes of a type. One common usage pattern, especially in C, is to use `sizeof` to determine the size of an array. However, arrays decay to pointers when passed as arguments to a function, and if `sizeof` is applied to such an argument, it will return the size of the pointer, not of the array. A similar issue happens when the array is used in an arithmetic operation.

This rule raises issues when:

- `sizeof` is used to compute the array size of a pointer passed as a function argument.
- `sizeof` is called on the result of an arithmetic operation involving an array.

Note: C++17 provides a `std::size` function that will correctly compute the number of elements of an array and fail to compile if provided with a pointer. It is simpler and safer to use this variant when available. C++20 also provides the functions `std::ssize`, `std::ranges::size`, and `std::ranges::ssize` with similar effects.

Noncompliant Code Example

```
void fun(int *data, int array[10]) {
  size_t const dataSize = sizeof data / sizeof(int); // Noncompliant, type of data is int *
  size_t const arraySize = sizeof array / sizeof(int); // Noncompliant, type of array is int * too
  int primes[] = { 1, 2, 3, 5, 7, 13, 17, 19};
  size_t const primesSize = sizeof primes / sizeof(int); // Compliant, type of primes is int[8]
  size_t const primesSize2 = sizeof(primes + 1) / sizeof(int); // Noncompliant, type of primes + 1 is int *
}
```

Compliant Solution

```
// Computing dataSize is now the responsibility of the caller
void fun(int *data, int dataSize int (&array)[10]) {
  size_t const arraySize = sizeof array / sizeof(int); // Compliant, no decay
  int primes[] = { 1, 2, 3, 5, 7, 13, 17, 19};
  size_t const primesSize = std::size(primes); // Better variant in C++17
  size_t const primesSize2 = sizeof primes / sizeof(int) + 1;
}
```

See

- CERT, ARR01-C. - Do not apply the `sizeof` operator to a pointer when taking the size of an array
- MITRE, CWE-467 - Use of sizeof() on a Pointer Type