Potentially unsafe call to strncat

Name: Potentially unsafe call to strncat

Description: Calling 'strncat' with the size of the destination buffer as the third argument may result in a buffer overflow.

ID: cpp/unsafe-strncat

Kind: problem

Severity: warning

Precision: medium

The standard library function `strncat` appends a source string to a target string. The third argument defines the maximum number of characters to append and should be less than or equal to the remaining space in the destination buffer. Calls of the form `strncat(dest, src, strlen(dest))` or `strncat(dest, src, sizeof (dest))` set the third argument to the entire size of the destination buffer. Executing a call of this type may cause a buffer overflow unless the buffer is known to be empty. Buffer overflows can lead to anything from a segmentation fault to a security vulnerability.

Recommendation

Check the highlighted function calls carefully to ensure that no buffer overflow is possible. For a more robust solution, consider updating the function call to include the remaining space in the destination buffer.

Example

```
1 strncat(dest, src, strlen(dest)); //wrong: should use remaining size of dest
2
3 strncat(dest, src, sizeof(dest)); //wrong: should use remaining size of dest.
4                                   //Also fails if dest is a pointer and not an array.
```

References

- cplusplus.com: strncat, strncpy.
- I. Gerg, *An Overview and Example of the Buffer-Overflow Exploit*. IANewsletter vol 7 no 4, 2005.
- M. Donaldson, *Inside the Buffer Overflow Attack: Mechanism, Method & Prevention*. SANS Institute InfoSec Reading Room, 2002.
- Common Weakness Enumeration: CWE-676.
- Common Weakness Enumeration: CWE-119.
- Common Weakness Enumeration: CWE-251.