strcpy() and strcat()

Daniel Plakosh, Software Engineering Institute [vita[1]]

Copyright © 2005 Pearson Education, Inc.

2005-09-27

The `strcpy()` and `strcat()` functions have been villainized as a major source of buffer overflows, and there are many mitigation strategies that provide more secure variants of these functions. However, not all applications of `strcpy()` are flawed.

Development Context

Copying and concatenating character strings

Technology Context

C, UNIX, Win32

Attacks

Attacker executes arbitrary code on machine with permissions of compromised process or changes the behavior of the program.

Risk

The strcpy() and strcat() functions are a source of buffer overflow vulnerabilities.

Description

The `strcpy()` and `strcat()` functions have been villainized as a major source of buffer overflows, and there are many mitigation strategies (such as `strcpy_s()` and `strcat_s()`) that provide more secure variants of these functions. However, not all applications of `strcpy()` are flawed. For example, assuming source has been properly validated, it is often possible to dynamically allocate the required space as follows:

```
dest = (char *)malloc(strlen(source) + 1);
if (dest) {
  strcpy(dest, source);
}
else { /* Handle memory allocation error */
  …
}
```

There are also other cases where it is clear that there is no potential for writing beyond the array bounds.

As a result, it may not be cost effective to replace or otherwise secure every call to `strcpy()`. This

1. daisy:268 (Plakosh, Daniel)

depends on the overall mitigation strategy adopted, as some strategies require an overall retooling of string manipulation logic.

References

[ISO/IEC 99] ISO/IEC. *ISO/IEC 9899 Second edition 1999-12-01 Programming languages — C.* International Organization for Standardization, 1999.

Pearson Education, Inc. Copyright

This material is excerpted from *Secure Coding in C and C++*, by Robert C. Seacord, copyright © 2006 by Pearson Education, Inc., published as a CERT® book in the SEI Series in Software Engineering. All rights reserved. It is reprinted with permission and may not be further reproduced or distributed without the prior written consent of Pearson Education, Inc.

Fields

Name	Value
Copyright Holder	Pearson Education

Fields

Name	Value
is-content-area-overview	false
Content Areas	Knowledge/Coding Practices
SDLC Relevance	Implementation
Workflow State	Publishable