Oscar Espinosa Curiel

Funciones vulnerables a Overflows y String Format en Cy su respectiva función segura.

Función vulnerable	Función	Función segura	Función
Strcpy (arg1, arg2)	Copia el Segundo argumento en el primero	`Strncpy(char *dest, const char *src, size_t n)`	Copia *n* caracteres de src en dest. Control de overflow por el tercer argumento
strcat(char *dest, const char *src)	Concatena src al final de dest.	`strncat(char *dest, const char *src, size_t n)`	Concatena n caracteres de src al final de dest.
gets(char *str)	Almacena una cadena dada desde stdin	`fgets(char *cadena, int n, FILE *stream)`	Lee n caracteres desde el archivo stream, y lo almacena en cadena.
sprintf(char *cadena, const char *formato, ...)	Escribe formato dentro de un array cadena, lo copia con cierto formato especificado.	`snprintf(char *str, size_t size, const char *format, ...)`	Escribe n caracteres de format dentro de str con el formato especificado.
printf(char *cadena, const char *formato, ...)	Imprime una cadena en stdout. Vulnerable cuando no se establece formato a cadena.	`printf(char *cadena, const char *formato, ...)`	No vulnerable cuando se establece el formato de cadena.
fprintf(FILE *stream, const char *format, ...)	Imprime cadena en el archivo stream. Vulnerable cuando no se establece formato a cadena.	`fprintf(FILE *stream, const char *format, ...)`	No vulnerable cuando se establece el formato de cadena.
sprintf(char *cadena, const char *formato, ...)	Almacena una cadena dentro de un array con cierto formato. Vulnerable cuando no se establece formato a cadena.	`sprintf(char *cadena, const char *formato, ...)`	No vulnerable cuando se establece el formato de cadena.

Fuentes:

https://stackoverflow.com/questions/26558197/unsafe-c-functions-and-the-replacement

https://www.owasp.org/index.php/Reviewing_Code_for_Buffer_Overruns_and_Overflows

https://security.web.cern.ch/security/recommendations/en/codetools/c.shtml