Funciones vulnerables

En la tabla 1 se muestran las funciones vulnerables a buffer overflow en C y con la función que soluciona el buffer overflow.

Tabla 1. Funciones Vulnerables a buffer overflow

Función vulnerable	Descripción	Función no vulnerable	Descripción
gets	La función no verifica la longitud del buffer	fgets	Asignación de memoria dinámicamente.
strcpy	La función no verifica la longitud del buffer y puede sobre escribir zonas de memoria contigua.	strlcpy	
		strncpy	Concatena los n bytes que se van a copiar para comprobar el tamaño de destino
strcat	La función no verifica la longitud del buffer y puede sobre escribir zonas de memoria contigua.	strncpm	Concatena la cadena a la cadena destino.
strcmp	La función no verifica la longitud del buffer y puede sobre escribir zonas de memoria contigua.	strncat	Compara los n bytes de las cadenas.
printf	Sin especificar el tipo de dato que se va a utilizar se puede sobreescribir la memoria.		
scanf	La función no verifica el tamaño del buffer por lo que puede sobre escribir zonas de memoria contigua.	snprintf	Lee la entrada estándar.

Referencias

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