Buffer Overflow

زمانی که مقدار بیشتری از ظرفیت بافر به آن اعمال شود اطلاعات در فضای بیرون از بافر نوشته می‌شود و اطلاعات قبلی از بین می‌رود. این تقریباً همیشه منجر به خرابی اطلاعات مجاور روی بافر می شود که می تواند منجر به خرابی برنامه ، عملکرد نادرست یا مشکلات امنیتی شود.

حملات سرریز بافر

حملات سرریز بافر زمانی رخ می‌دهند که نفوذگری اقدام به انجام سرریز بافر می کند. این حمله جزء خطرناک‌ترین حملات حساب می‌شود و اکثر نفوذگران به قصد حمله به سیستم عامل از این آسیب‌پذیری بهره می‌برند.

زبان‌های برنامه نویسی ای مانند C و C++ بدلیل اینکه اجازه دسترسی مستقیم به فضاهای حافظه را می دهند و شیء از نوع قوی (strong object types) در آن ها وجود ندارد، به راحتی دچار حملات سرریز بافر می‌شوند و کنترل دسترسی حافظه به دست نفوذگر می‌افتد.

روش های جلوگیری

فضا های آدرس با چیدمان تصادفی (ASLR-Address Space Layout Randomization)

مکان فضاهای آدرس که داده‌های مهمی در آن قرار می‌گیرد، بصورت تصادفی انتخاب شود. با توجه به آن‌که دانستن محل دقیق این فضاها برای اجرای کد مخرب مهم هست، با این کار دیگر شاهد حملات سرریز بافر نخواهیم بود.

بررسی مرزها (Bounds Checking) و عدم استفاده از توابع کتابخانه ای استاندارد که حجم بافر را بررسی نمی‌کنند احتمال وقوع حملات سرریز بافر را کاهش می‌دهد.

استفاده از مقادیر قناری (Canaries)

قناری ها یا کلمات قناری مقادیر شناخته شده ای هستند که برای نظارت بر سرریز بافر بین یک بافر و داده های کنترل روی پشته قرار می گیرند. در زمان سرریز بافر، معمولاً اولین داده‌ای که خراب می‌شود مقدار قناری است. پس از خرابی مقدار قناری هشدار سرریز بافر منتشر می‌شود و سپس می‌توان این خطا را مدیریت کرد. سه نوع کلمات قناری به سه نوع خاتمه‌دهنده(Terminator canaries)، تصادفی (random canaries) و XOR تصادفی (Random XOR) تقسیم می شوند.