Kohl Johnson

CST-321

01-24-2025

Security Research

# Buffer Overflow

A buffer overflow is an anomaly where a program attempts to write data to a buffer beyond the allocated memory, which then overwrites adjacent memory locations. Buffers are areas of memory that are set aside to hold/store data while moving through a program or even from program to program. Overflows are often triggered by bad inputs. For example, if a programmer assumes that all inputs will be smaller than X size and created the buffer to be that said size, then an overflow would be in an input that is greater than that said size and writes past the end of the buffer. In doing so, it overwrites adjacent data or executable code which can cause unplanned program behavior like memory access errors, incorrect outputs, and crashes.

The exploitation of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program (or system as a whole) is well defined and planned. By purposely sending data to cause a buffer overflow, it is possible to overwrite areas known to hold executable code with malicious code to cause behavior that was not intended by the original developer.

A grid with green squares and black letters

Description automatically generated

# Zero-Day Exploit

A zero-day exploit is a vulnerability in software that is usually unknown to the developer and therefore has no patch or fix available. With that in mind, the developer has zero days to prepare the said patch, as the vulnerability has already been discovered and/or exploited. Despite a developer’s goal of delivering a secure product that functions as desired, virtually all software and hardware contain bugs. Many of these impair the security of the system and are therefore known as vulnerabilities. Although zero-day vulnerabilities are a small percentage of overall cyberattacks, they are considered more dangerous than known vulnerabilities because there are fewer countermeasures possible.

# Kali Linux

Kali Linux is a Debian-based Linux distribution that allows users to perform advanced penetration testing and security audits. It runs on multiple platforms and is freely available to both information professionals and hobbyists. The distribution itself contains hundreds of tools, configurations, and scripts with industry-specific modifications to allow users to focus on tasks like reverse engineering, vulnerability detection, and computer forensics. Some of the notable features include an open source Git tree, custom kernel, GPG signed packages (meaning each individual developer signs the package), multi-language support, ARMEL and ARMHF support, and free to use.

# Password Checker

# A screenshot of a computer Description automatically generated

# User Management

**No submission, ran out of time.**