Joey Navarrete
CYSE 462: Cybersecurity Fundamentals
10/27/2022

Module 10: Assignment

Resource Leak

A resource leak can be defined as a consumption of resources by a computer in which it does not release the acquired resources. A resource leak can be fixed through resource management, which is capable of preventing leaks by immediately releasing resources. Resource leaks can be prevented through: Restarting your computer, using Windows Memory Diagnostic to fix leak, disabling startup programs, updating device drivers, and running an antivirus scan to get around the problem (Online Tech Tips).

Incorrect Usage of APIs

The incorrect usage of APIs can happen when "the application does not conform to the API requirements for a function call that requires extra privileges. This could allow attackers to gain privileges by causing the function to be called incorrectly." (Common Weakness Enumeration). There are multiple ways that this issue can be fixed, or, in this case, prevented. One way is to "ensure that the assumptions made by the privileged code hold true prior to making the call." (Common Weakness Enumeration). Another good thing to do is to "only call privileged APIs from safe, consistent and expected state." (Common Weakness Enumeration).

Insecure Data Handling

Insecure data handling can happen when data is not properly or securely stored on a device. This usually occurs when the data is accessible to outsiders, or those who are capable of attacking data. Many phone apps are vulnerable to insecure data handling, as

they may not be as secure as they should be. To combat this, there is a list of measures that can be taken to prevent insecure data handling. This includes: “URL caching, keyboard press caching, copy/paste buffer caching, application backgrounding, intermediate data, logging, HTML5 data storage, browser cookie objects, and analytics data sent to 3rd parties.” (OWASP).

Buffer Overflow

Buffer overflows often happen to buffers, which are “memory storage regions that temporarily hold data while it is being transferred from one location to another.” (Imperva). They usually happen from mis-inputs or “failure to allocate enough space for the buffer.” (Imperva). Buffer overflow attacks usually happen when an attacker overrules an application’s memory, which usually leads to damaged files. There are three different ways that buffer overflows can be prevented. The first way is by address space randomization, also known as ASLR. What this does is it “randomly moves around the address space locations of data regions.” (Imperva). The next way is data execution prevention, which “flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.” (Imperva). The last measure that can be taken is Structured Exception Handler Overwrite Protection, or SEHOP. The job of this is that it “helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions.” (Imperva).

Use of Uninitialized Data

The use of uninitialized data or memory “means reading data from the buffer that was allocated but not filled with initial values.” (PVS-Studio). There are multiple fixes to this. The first one is to “attack surface reduction” and “assign variables to initial value.” (CWE). Another fix is to “run or compile the software in a mode that reports undeclared or unknown variables.” (CWE).

Joey Navarrete
CYSE 462: Cybersecurity Fundamentals
10/27/2022

References

Buffer Overflow Attack https://www.imperva.com/learn/application-security/buffer-overflow/

CWE-457: Use of Uninitialized Variable
https://cwe.mitre.org/data/definitions/457.html

CWE-648: Incorrect Use of Privileged APIs
https://cwe.mitre.org/data/definitions/648.html

How to fix Windows 10 Memory Leaks https://www.online-tech-tips.com/windows-10/how-to-fix-windows-10-memory-leaks/

M2: Insecure Data Storage https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage

Use of uninitialized memory https://pvs-studio.com/en/blog/terms/0079/#:~:text=Use%20of%20uninitialized%20memory%20means,a%20so%20called%20%22heisenbug%22.