23/8/15

Principles of Information Security
Assignment 1

1) Hardware : CVE-2023-40238 (logoFAIL)

logofail is a major vulnerability that was discovered in UEFI firmware based implementations used by many modern motherboards. UEFI (United Extensible Firmware Interface) is the system firmware that runs before the operating system starts. It is responsible for initializing hardware and handeling control to the operating system.

The flaw. (CVE-2023-40238) specifically affects firmware based on TianoCore EDK II, which is used by vendors like Insyde H2O, AMI Aptio, and Phoenix. LogoFAIL occurs because the firmware loads and displays vendor logos from storage during startup. Researchers found that these logos files were not properly validated. By replacing the legitimate boot logo with a maliciously crafted image, attackers could trick the firmware into executing arbitrary code at the earliest stage of boot.

* This type of vulnerability is dangerous because :-

- It occurs before the operating system starts, meaning normal antivirus cannot detect or stop it -

- Attackers can achieve persistence - the malicious code stays even after reinstalling the operating system.
- Since firmware operates at the lowest level, attackers can bypass secure boot and security tools.

Impact:- Devices running vulnerable firmware can be completely taken over, making it possible to install rootkits or spyware that are nearly impossible to detect.

---

2. Operating System : CVE - 2025 - 21362 (Linux kernel eBPF Vulnerability)

It is a critical privilege ~~es esc~~ esclation vulnerability discovered in the Linux kernel's eBPF subsystem. eBPF (extended Berkeley packet filter) is a technology that allows you to run programs in kernel for networking, tracing and security purposes.

The flaw affects linux kernel versions 5.15 to 6.6. The vulnerability exists in the eBPF verifier, which is supposed to check the safety of user-supplied eBPF programs before running them in kernel. However, due to a flaw in type safety verification, an attacker could craft a malicious eBPF program that bypasses checks and manipulates kernel memory.

* Impact :-

- A local attacker with permission to run eBPF programs (often available to normal users on many linux distributions) could exploit this bug to gain root privileges.

- It allows complete system compromise, bypassing sandboxing and kernel protections.

- Attackers can disable security frameworks like SE linux or APP Armour, making the system completely vulnerable.

* Mitigation :- linux developers patched this vulnerability in kernel 6.6.1 and above. Distributions have released backported fixes as well.

---

3. Web Application : CVE-2025-26615 (WeGIA Path Traversal)

It is a vulnerability found in WeGIA, which is an opensource web-based system for managing institutions (used for scheduling, information systems and database-backend applications).

The flaw lies in its examples.php endpoint which failed to properly validate user input.

The issue is a classic path traversal vulnerability. Path traversal occurs when attackers manipulates file paths in input parameters (for eg: ../../etc/passwd) to access files outside the intended directory.

In WeGIA, this allowed attackers to access sensitive configuration files like config.php That file often contains critical data such as database usernames, passwords and system configuration values.

* Impact:-

- By exploiting this vulnerability, an attacker can steal credentials and gain unauthorized access to the application's database.

- It may also lead to data breaches manipulation of records, or even full application compromise if the attacker escalates privileges.

- Since it is accessible over the web, attackers can exploit this remotely without needing local access.

* Mitigation:-

The developers of WeGIA fixed this vulnerability in version 3.2.14. users of the application should upgrade to this version immediately.

Additionaly, best practices such as using parameter sanitization, web application firewalls (WAFs) and monitoring server logs can reduce the risk of exploitation.

4. Software : CVE - 2025 - 27363 (Free Type library vulnerability)

It is a high-severity vulnerability (CVSS Score 8.1) that was discovered in the Free Type library. Free type is an open source library used to render text on screen, especially for displaying fonts in applications, web browsers, operating systems, and embedded devices.

The vulnerability exist in versions up to Free Type 2.13.0 It is an out-of-bounds write vulnerability, which means the program writes data past the allocated memory buffer. when a user or system processes a maliciously crafted font file, this flaw can be triggered. Because Free Type is used widely by applications that handle font font rendering (like Chrome, firefox, linux desktop environments and even game engines), exploitation can allow an attacker to execute arbitrary code.

*** Impact :-**

- If an attacker convinces a user to open or display a specially crafted font, the attacker could run malicious code with the previleges of the user
- It can lead to system crashes.

*** Mitigation :-**

users and ~~ap~~ administrators are advised to update to to Free Type 2.13.3 or later, which fixes the vulnerability.