**Module 1 Threats, Attacks & Vulnerabilities**

**1.6 Impacts Associated with Types of Vulnerabilities**

**Vulnerability Types**

* Race Condition (Race Hazard)

1. Behaviour of electronics/software/system where output dependent on sequence/timing of other uncontrollable events
2. When events don’t happen in order programmer intended

* Improper Input Handling

1. When system doesn’t validate input properly, attacker able to craft input in form that isn’t expected by rest of app
2. Lead to parts of system receiving unintended input, which may result in altered control flow/arbitrary control of a resource/arbitrary code execution

* Improper Error Handling – when system generates error message that includes sensitive information about its environment, users or associated data
* Misconfiguration/Weak Configuration

1. Using insecure configuration/control settings
2. Eg. Browsers, System Policies (Windows GPOs), Wi-Fi

* Default Configuration – often systems/devices/software distributed with insecure default settings
* Weak Cipher Suites

1. Use of older/less robust cryptographic algorithms for encrypting data
2. Eg. DES, WEP

* Improper Certificate & Key Management

1. Allowing unauthorised access to encryption keys/certificates
2. Allows sensitive data to be decrypted
3. Also allowing digital certificates to expire

* Improperly Configured Accounts – accounts have greater privileges than needed to perform function. Solved by Least Privilege
* Resource Exhaustion – simple DoS condition that happens when resources required to execute action entirely expended, preventing action from occurring
* Vulnerable Business Processes (AKA Business Process Compromise) – silently altering parts of specific business processes/machines facilitating these processes to gain access to systems/generate monetary profit for attackers
* System Sprawl/Undocumented Assets

1. Allowing unchecked systems/devices on internal network
2. Lack of internal inventory system

* Architecture/Design Weaknesses

1. Insecurely designed network/system architecture
2. Eg. Not segmenting systems on internal network

* Vulnerabilities due to

1. End-of-Life (EOL) systems
2. Embedded systems
3. Lack of vendor support

* Memory/Buffer Vulnerability

1. Memory Leak
2. Integer Overflow
3. Buffer Overflow
4. Pointer Deference
5. DLL Injection