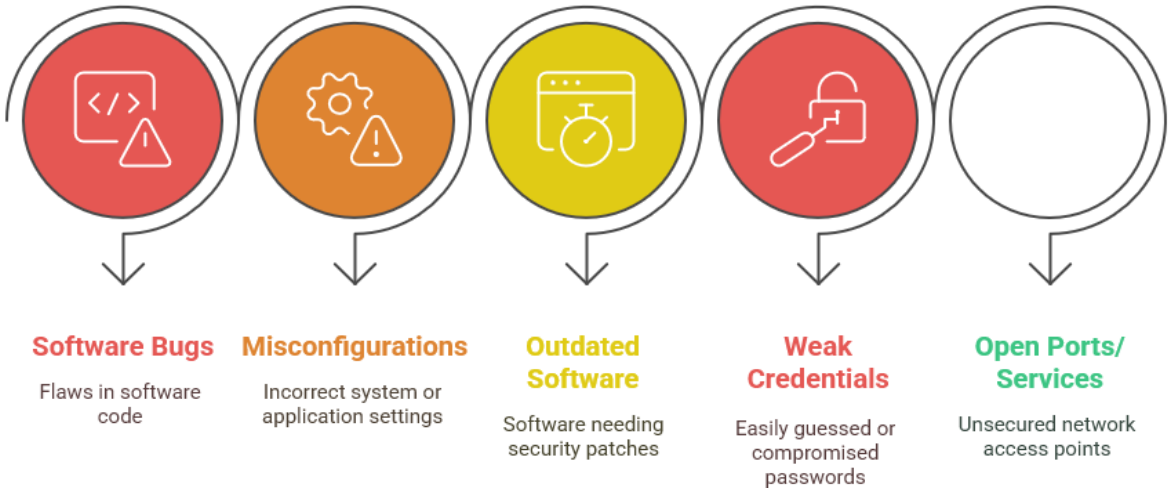
Vulnerability:

A **vulnerability** is a **weakness or flaw** in a computer system, network, application, or configuration that could be **exploited by a threat actor** like a hacker to compromise confidentiality, integrity, or availability. A vulnerability is not an attack, but an opportunity for an attack. When exploited, it can lead to data breaches, system compromise, malware infection, or denial of service. Vulnerability such as Software Bugs, Misconfigurations, Outdated Software, Weak Credentials, Open Ports/Services.



1. EternalBlue (CVE-2017-0144)

- **Type:** Remote Code Execution (RCE)
- **Affected Systems:** Microsoft Windows (SMBv1 protocol)
- **Discovered By:** NSA (leaked by Shadow Brokers)
- **Exploited In:** WannaCry ransomware, NotPetya worm
- **Impact:** Millions of systems affected worldwide; major organizations shut down
- **Mitigation:** Apply Microsoft patch MS17-010, disable SMBv1

2. Heartbleed (CVE-2014-0160)

- **Type:** Information Disclosure
- **Affected Systems:** OpenSSL 1.0.1–1.0.1f
- **Exploit:** Leaked memory contents from servers, including credentials and keys
- **Impact:** Major sites like Yahoo and others were vulnerable
- **Mitigation:** Update OpenSSL, regenerate SSL certificates

3. Log4Shell (CVE-2021-44228)

- **Type:** Remote Code Execution in Apache Log4j 2
- **Affected Systems:** Java applications using vulnerable versions of Log4j
- **Exploited In:** Cloud services, Minecraft servers, enterprise apps
- **Impact:** Allowed attackers to run arbitrary code by logging a crafted string
- **Mitigation:** Update Log4j to a patched version, use JNDI lookups mitigations