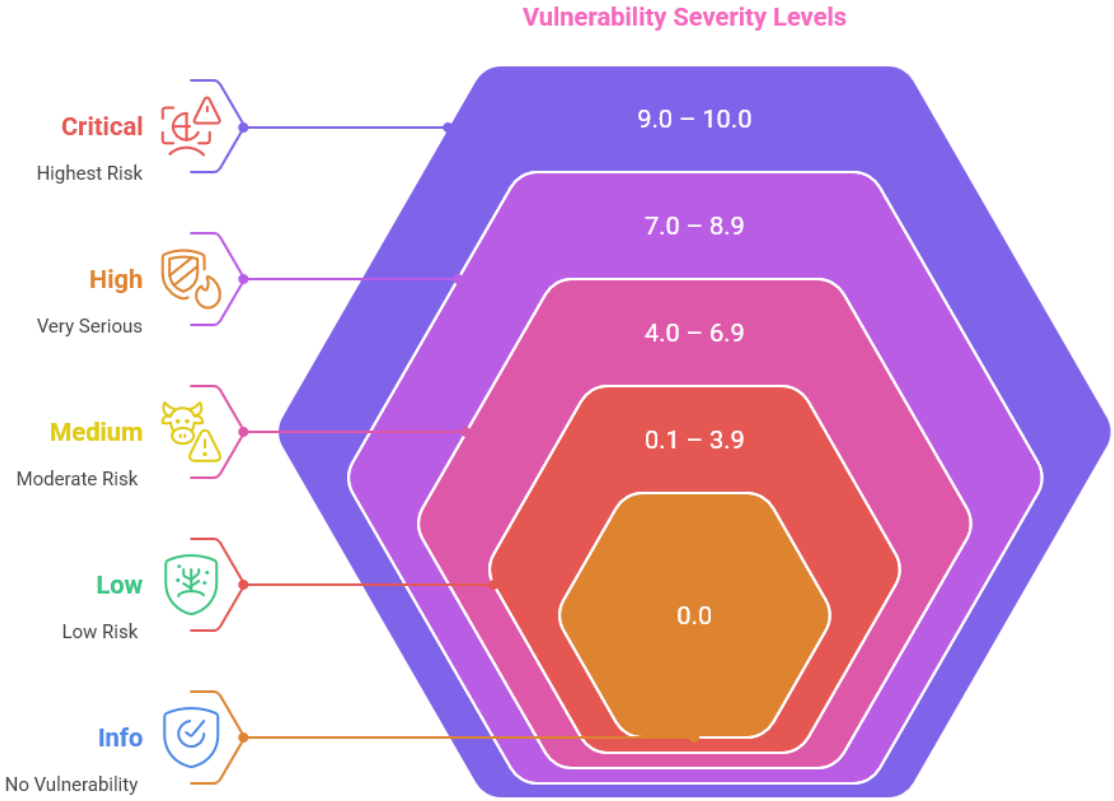
Understanding Severity Levels:

In **Nessus**, vulnerabilities are assigned **severity levels** to help you prioritize which issues to fix first. These levels are based on how dangerous a vulnerability is and how easily it can be exploited. Severity levels in Nessus indicate the risk posed by a vulnerability, based on factors like its potential to be exploited, the damage it could cause, and the ease of exploitation.



1. Critical

- **Highest risk, CVSS Score: 9.0 – 10.0**
- Represents the most severe vulnerabilities.
- Exploits are often publicly available and actively used by attackers.
- Can be easily exploited by attackers to **take full control** of a system.
- Usually requires **immediate action**

Examples:

- Remote Code Execution (RCE)
- Known exploits available in the wild
- Default admin passwords exposed

Fix these immediately.

2. High

- **Very serious**, **CVSS Score**: **7.0 – 8.9**
- It is slightly less urgent than Critical
- Can lead to **privilege escalation**, **data loss**, or **denial of service**
- May require some conditions to be met before exploitation
- Weak credentials or default passwords on critical systems.
- Potential for unauthorized access, data theft, or service outages.

Examples:

- SQL Injection
- Outdated software with known exploits
- Weak SSH configuration

Fix these as soon as possible.

3. Medium

- **Moderate risk, CVSS Score: 4.0 – 6.9**
- Exploits may be harder to perform or have limited impact
- Useful for attackers to gather more info for larger attacks

Examples:

- Information disclosure
- Clickjacking
- Missing HTTP security headers

Fix within a reasonable time frame.

4. Low

- **Low risk** vulnerabilities, **CVSS Score**: **0.1 – 3.9**
- Unlikely to be exploited or cause damage
- Often **best practices** or **informational warnings**

Examples:

- Expired SSL certificate
- Open port with no vulnerable service
- Outdated software with no known exploit

Monitor and fix when convenient.

5. Info

- **No vulnerability, CVSS Score: 0.0**
- These findings **do not pose an immediate security risk**
- They **describe system behavior, configurations, or open services**
- Useful for **network mapping, asset discovery**, or **baseline documentation**

Severity	Risk Level	Action Timeframe	Example
Critical	Extremely High	Fix **immediately**	RCE, default creds, wormable exploits
High	High	Fix **ASAP**	SQLi, privilege escalation
Medium	Medium	Fix in **scheduled patch**	Info leaks, missing headers
Low	Low	Fix **when possible**	Expired cert, unused open port

Level	Color	Impact	Action
Critical	Red	Severe threat	Fix immediately
High	Orange	Serious risk	Fix as soon as possible
Medium	Yellow	Moderate	Fix in patch cycle
Low	Green	Minor risk	Fix when possible
Informational	Blue	No risk	Review for insight and documentation