Cybersecurity Vulnerability Management Overview

# What is CVE?

CVE (Common Vulnerabilities and Exposures) is a unique identifier for publicly known cybersecurity vulnerabilities.  
- Managed by: MITRE Corporation  
- Format: CVE-2025-12345  
- Purpose: Standardized naming of vulnerabilities to simplify sharing across tools, vendors, and researchers.

# What is CVSS?

CVSS (Common Vulnerability Scoring System) provides a numerical score (0.0–10.0) and severity rating (Low, Medium, High, Critical).  
Example Severity Ratings:  
- Low: 0.1–3.9  
- Medium: 4.0–6.9  
- High: 7.0–8.9  
- Critical: 9.0–10.0  
Components:  
- Base score (severity)  
- Temporal score (evolving threat)  
- Environmental score (impact on specific system)

# What is CWE?

CWE (Common Weakness Enumeration) is a classification system for software vulnerability types.  
Examples:  
- CWE-79: Cross-Site Scripting (XSS)  
- CWE-89: SQL Injection

# How Are CVEs Classified?

Based on CVSS score and impact, vulnerabilities are classified as:  
- Low: Minimal risk  
- Medium: Needs attention, not urgent  
- High: Can cause major damage  
- Critical: Immediate fix required; can be exploited remotely, no user interaction

# Once Vulnerability is Identified – How to Fix It?

1. Validate the finding  
2. Assess the risk  
3. Check vendor advisories  
4. Apply the fix (patch, config changes, access restrictions)  
5. Test after remediation  
6. Document and monitor

# How to Prioritize Critical and High Vulnerabilities

1. Use risk-based approach (CVSS ≥ 7, public exploit, critical assets)  
2. Patch immediately or within SLA  
3. Monitor for exploitation attempts  
4. Use compensating controls if no patch available

# Recommendations to Fix Vulnerabilities

- Patch the affected system  
- Upgrade to secure versions  
- Disable unused services  
- Sanitize user inputs  
- Harden configurations  
- Use security tools (WAF, IDS, EDR)  
- Developer/admin training

# What is a Zero-Day Vulnerability?

A zero-day vulnerability is a flaw unknown to the vendor with no patch available.  
Often exploited in the wild before detection; highly dangerous.

# How to Identify POC (Proof of Concept) for a CVE

Search platforms:  
- Exploit-DB  
- GitHub  
- Packet Storm  
- Metasploit  
- CVE Details  
Example search: CVE-XXXX-YYYY site:github.com

# Top 5 Security Websites

1. Krebs on Security - https://krebsonsecurity.com  
2. The Hacker News - https://thehackernews.com  
3. Bleeping Computer - https://www.bleepingcomputer.com  
4. Exploit-DB - https://www.exploit-db.com  
5. NVD - https://nvd.nist.gov

# Top Twitter/X Feeds to Follow

1. @briankrebs  
2. @thehackersnews  
3. @cyberwar  
4. @MalwareTechBlog  
5. @0xAmit