DROP.ORG.IN

DCSC Training

Unlock Success with Alumni Stories You Can't Ignore

Ethical Hacking

Version 2.0

droporganization@gmail.com

www.drop.org.in

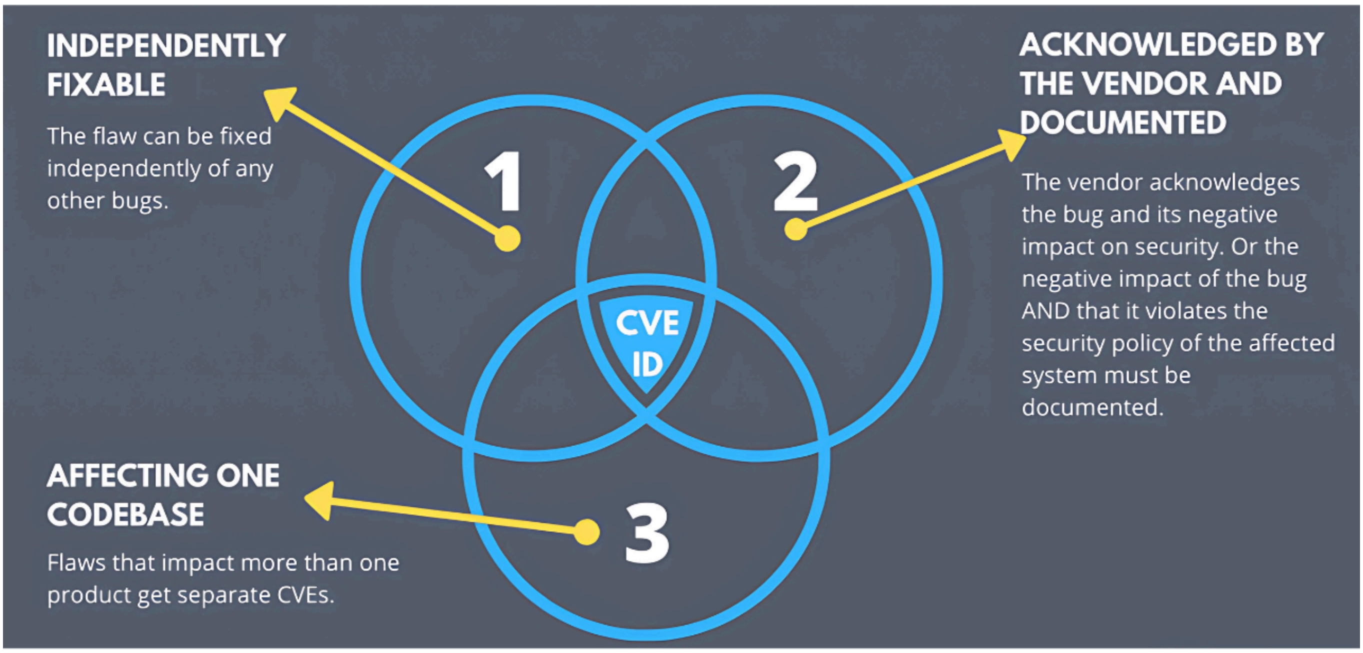
Lesson 08: Common Vulnerabilities and Exposures (CVE)

Lesson Objectives

By the end of this lesson, students will be able to:

- Understand what Common Vulnerabilities and Exposures (CVE) are.
- Learn the importance of CVE in cybersecurity.
- Identify how CVEs are reported, classified, and managed.
- Explore the impact of CVEs on organizations and individuals.
- Understand best practices for mitigating vulnerabilities.

1. Introduction to CVE


INDEPENDENTLY FIXABLE
The flaw can be fixed independently of any other bugs.
1
2
ACKNOWLEDGED BY THE VENDOR AND DOCUMENTED
The vendor acknowledges the bug and its negative impact on security. Or the negative impact of the bug AND that it violates the security policy of the affected system must be documented.
CVE ID
AFFECTING ONE CODEBASE
Flaws that impact more than one product get separate CVEs.
3

Common Vulnerabilities and Exposures (CVE) is a publicly available list of known cybersecurity vulnerabilities. It helps security professionals and organizations identify, categorize, and address security flaws in software and hardware.

2. Importance of CVE in Cybersecurity

- Provides a standardized way to identify vulnerabilities.
- Helps security teams prioritize and address security flaws.
- Enables organizations to stay updated on emerging threats.
- Supports vulnerability management and patching efforts.
- Facilitates better collaboration between security researchers and vendors.

3. How CVEs are Reported and Classified

3.1 CVE Reporting Process

1. A security researcher discovers a vulnerability.
2. The researcher reports the vulnerability to a CVE Numbering Authority (CNA) or vendor.
3. The vulnerability is analyzed, verified, and assigned a CVE ID.
4. The CVE entry is published in the CVE database.

3.2 CVE Classification and Scoring

- **Common Vulnerability Scoring System (CVSS)**: A framework for assessing the severity of CVEs.
- CVSS score ranges:
    - **Low (0.1 - 3.9)**: Minor impact on systems.
    - **Medium (4.0 - 6.9)**: Noticeable security risks.
    - **High (7.0 - 8.9)**: Significant security concerns.
    - **Critical (9.0 - 10.0)**: Severe threats requiring immediate action.

4. Impact of CVEs on Organizations and Individuals

- **Organizations**: Unpatched vulnerabilities can lead to data breaches, financial losses, and reputational damage.
- **Individuals**: Exploited vulnerabilities can result in identity theft, malware infections, and unauthorized access to personal data.

5. Mitigating CVEs and Best Practices

- Regularly update and patch software and hardware.
- Conduct vulnerability assessments and penetration testing.
- Monitor security advisories and subscribe to CVE databases.
- Implement multi-layered security controls (firewalls, IDS/IPS, etc.).
- Train employees on cybersecurity awareness and best practices.

6. Case Studies: Real-World CVE Incidents

- **CVE-2017-0144 (EternalBlue):** Exploited by WannaCry ransomware.
- **CVE-2021-44228 (Log4Shell):** A severe remote code execution vulnerability.
- **CVE-2014-0160 (Heartbleed):** A major OpenSSL vulnerability exposing sensitive data.

7. Summary and Key Takeaways

- CVEs are essential for tracking and managing security vulnerabilities.
- The CVE system provides transparency and helps organizations prioritize security efforts.
- Regular security updates and best practices help mitigate risks associated with CVEs.

8. Quiz & Discussion Questions

1. What is the purpose of the CVE system?
2. How does the CVE reporting process work?
3. What is the CVSS, and how does it help assess vulnerabilities?
4. Give an example of a real-world CVE and its impact.
5. What measures can organizations take to mitigate CVEs?

Visite For CVE :- https://cve.mitre.org/index.html