Tutorial No. 8

Title: Comprehrnding CERT, MITRE framework, CVSS for Ethical Disclosure

Roll No.: 16010423076 **Tutorial No.:8**

Aim: Comprehrnding CERT, MITRE framework, CVSS for Ethical Disclosure

---

Resources :

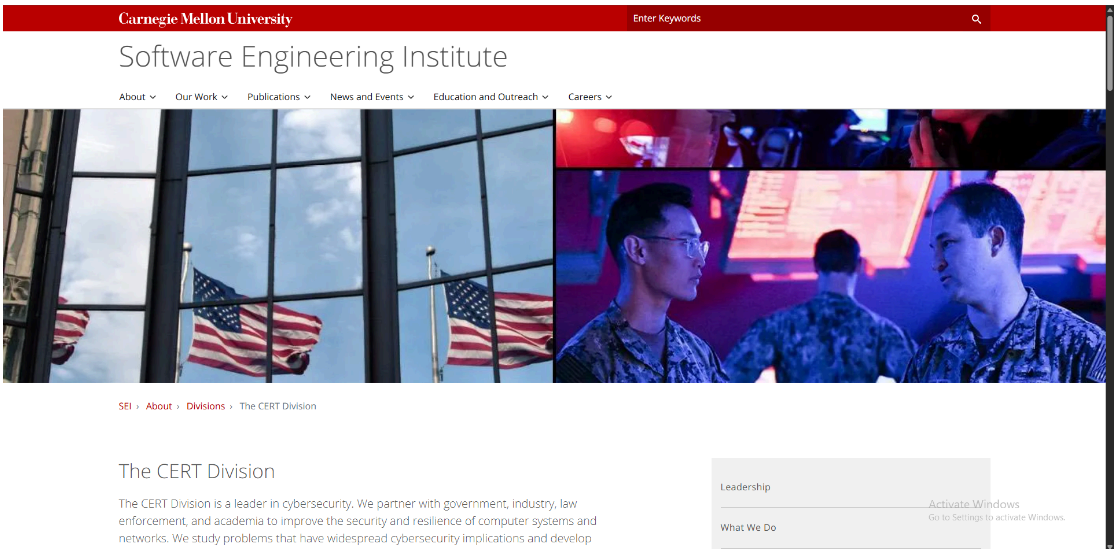
CERT Guide to Coordinated Vulnerability Disclosure
MITRE ATT&CK Framework
CVSS v4.0 Specification Document

Theory:

1. **Explain how frameworks like CERT, MITRE, and CVSS support responsible and transparent practices in vulnerability management and incident response**.

   Frameworks like CERT, MITRE, and CVSS are essential in promoting responsible and transparent practices in vulnerability management and incident response. They provide structured methodologies for identifying, assessing, and mitigating vulnerabilities, ensuring that all stakeholders are informed and can take appropriate actions.

2. **Discuss CERT's Role in Ethical Disclosure**



Carnegie Mellon University
Enter Keywords
Software Engineering Institute
About
Our Work
Publications
News and Events
Education and Outreach
Careers
SEI › About › Divisions › The CERT Division

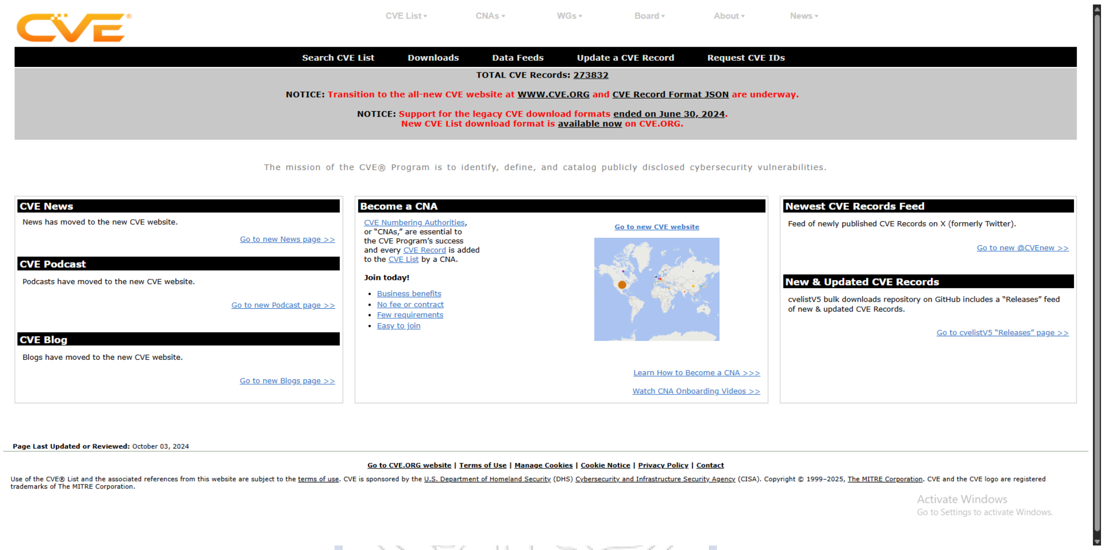
The CERT Division

The CERT Division is a leader in cybersecurity. We partner with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks. We study problems that have widespread cybersecurity implications and develop

Leadership
What We Do
Activate Windows
Go to Settings to activate Windows.

CERT (Computer Emergency Response Team) plays a pivotal role in ethical vulnerability disclosure through its Coordinated Vulnerability Disclosure (CVD) process. This process involves collaborating with stakeholders such as vendors, researchers, and coordinators to remediate or mitigate security vulnerabilities and minimize harm associated with disclosure. By adhering to principles like reducing harm and maintaining trustworthiness, CERT ensures that vulnerabilities are disclosed responsibly, balancing the need for public awareness with the potential risks of premature exposure.

3. **Elaborate on how MITRE frameworks aid in identifying, categorizing, and disclosing vulnerabilities ethically.**



TOTAL CVE Records: 273832

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.
New CVE List download format is available now on CVE.ORG.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs have moved to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Go to new CVE website

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records Feed

Feed of newly published CVE Records on X (formerly Twitter).

Go to new @CVEnew >>

New & Updated CVE Records

cvelistV5 bulk downloads repository on GitHub includes a "Releases" feed of new & updated CVE Records.

Go to cvelistV5 "Releases" page >>

Page Last Updated or Reviewed: October 03, 2024

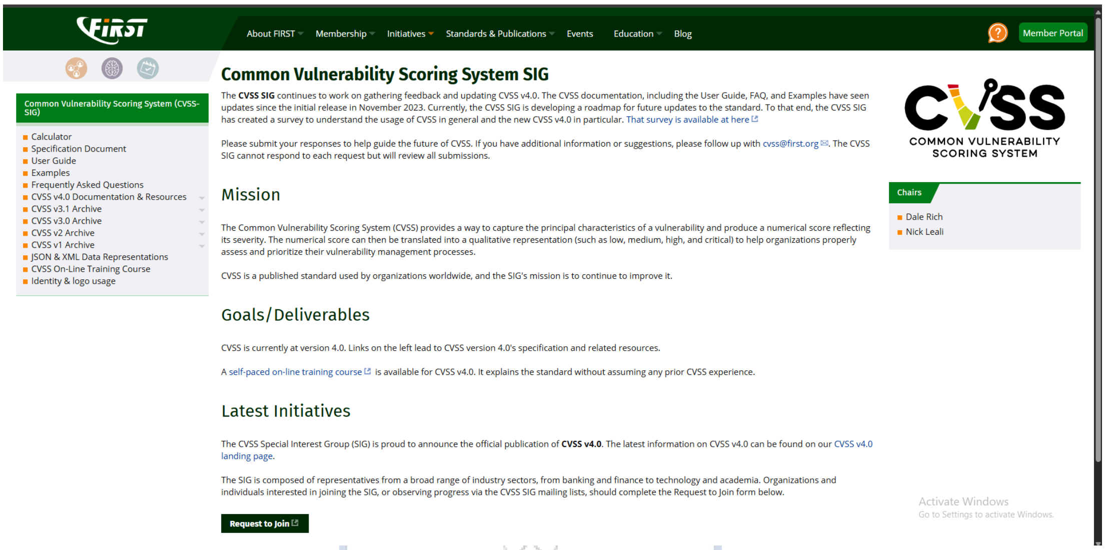
Go to CVE.ORG website | Terms of Use | Manage Cookies | Cookie Notice | Privacy Policy | Contact

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2025, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

Activate Windows
Go to Settings to activate Windows.

The MITRE ATT&CK framework is a comprehensive knowledge base that categorizes and describes adversary tactics and techniques based on real-world observations. By providing a common language for understanding attacker behaviors, it assists organizations in identifying and categorizing vulnerabilities within their systems. This structured approach enables defenders to anticipate potential attack vectors and implement appropriate mitigations. Furthermore, by openly sharing this information, MITRE promotes transparency and collaboration within the cybersecurity community, facilitating ethical disclosure and collective defense.

4. **How organizations can use CVSS scores to communicate vulnerability risks to stakeholders in an ethical and transparent manner?**



Common Vulnerability Scoring System SIG

The **CVSS SIG** continues to work on gathering feedback and updating CVSS v4.0. The CVSS documentation, including the User Guide, FAQ, and Examples have seen updates since the initial release in November 2023. Currently, the CVSS SIG is developing a roadmap for future updates to the standard. To that end, the CVSS SIG has created a survey to understand the usage of CVSS in general and the new CVSS v4.0 in particular. That survey is available at here

Please submit your responses to help guide the future of CVSS. If you have additional information or suggestions, please follow up with cvss@first.org. The CVSS SIG cannot respond to each request but will review all submissions.

Mission

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

Goals/Deliverables

CVSS is currently at version 4.0. Links on the left lead to CVSS version 4.0's specification and related resources.

A self-paced on-line training course is available for CVSS v4.0. It explains the standard without assuming any prior CVSS experience.

Latest Initiatives

The CVSS Special Interest Group (SIG) is proud to announce the official publication of **CVSS v4.0**. The latest information on CVSS v4.0 can be found on our CVSS v4.0 landing page.

The SIG is composed of representatives from a broad range of industry sectors, from banking and finance to technology and academia. Organizations and individuals interested in joining the SIG, or observing progress via the CVSS SIG mailing lists, should complete the Request to Join form below.

The Common Vulnerability Scoring System (CVSS) provides a standardized method for assessing the severity of software vulnerabilities. By assigning numerical scores, organizations can objectively communicate the potential impact of vulnerabilities to stakeholders. This transparency allows stakeholders to understand the risk landscape and prioritize remediation efforts accordingly. Ethically, using CVSS scores ensures that risk assessments are consistent and unbiased, fostering trust among stakeholders and promoting informed decision-making.

Outcomes: CO1: Realize that premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Through this tutorial, I gained insights into the roles of CERT, MITRE, and CVSS in ethical vulnerability management. CERT's CVD process emphasizes collaboration and harm reduction, ensuring responsible disclosure. The MITRE ATT&CK framework aids in systematically identifying and categorizing adversary techniques, enhancing our defensive strategies. Additionally, CVSS provides a standardized approach to quantify and communicate vulnerability severity, promoting transparency and informed decision-making among stakeholders.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

CERT Guide to Coordinated Vulnerability Disclosure: https://certcc.github.io/CERT-Guide-to-CVD/

MITRE ATT&CK Framework: https://attack.mitre.org/

CVSS v4.0 Specification Document: https://www.first.org/cvss/v4-0/specification-document