A Guide for Utilizing Common Vulnerability and Exposures for Threat Management in Cybersecurity

Prepared By:

Kimmie DeBolt

October 1st, 2024

Table of Contents

PREFACE **3**

Content Overview: 3

Purpose for Audience: 3

Assumptions of Audience: 3

Organization: 4

Tips for the Guide: 4

RESOURCES **5**

The Information Systems Audit and Control Association Journal 5

The Infosecurity Magazine 6

Gov Cybersecurity & Infrastructure Security Agency 7

The CVE Program 8

CVE Details 9

National Vulnerability Database (NVD by NIST) 10

Preface

Content Overview:

The guide below is an informational resource to be referenced regarding Common Vulnerability and Exposures within the field of cybersecurity. The resources provided includes cloud computing and cybersecurity journals such as *ISACA*, risk and threat management guides, databases, and a government publication. These resources share information regarding risk and threat management and can be used by those who are active in the cybersecurity frameworks. The magazines, journals, and government publications are to be employed for staying up to date on all the new attack surfaces and dangers that are always present. The databases are an excellent resource when the specific threat has been identified and the user is in search of mitigating factors or relevant patches.

Purpose for Audience:

The purpose of this guide is to assist those who are interested or involved in the field of cybersecurity. From students to professionals, there is something useful in this guide for everyone. The reservoir of information found here will aid users in taking a proactive approach when researching cybersecurity vulnerabilities. Users will be able to institute unique and effective risk/threat management techniques to protect their digital data against susceptibilities. This guide also supplies tips to support the user's navigation of the resources provided as well as their understanding. Ultimately, this guide compiles resources with the goal of aiding the user in strengthening their security posture against the forever evolving threat landscape within cybersecurity.

Assumptions of Audience:

This guide was not created with the intent of providing those unfamiliar with threat and risk management to become versed within the landscapes of common vulnerabilities and exposures. This guide assumes its readers have some extent of applicable cybersecurity knowledge specifically centered around vulnerabilities, exploits, various types of malwares, threat actors, and the CVSS system. Readers without knowledge of the previously listed items may have difficulty grasping concepts discussed as the details shared are not entry level. It is also assumed that the audience is familiar with industry definitions and vocabulary. Of course, new learners should not be discouraged from exploring their interests within this guide and are encouraged to do so.

Organization:

This guide is organized by journals and magazines, a government publication, and databases and directories. This is intentional as to go in order of increasing difficulty. While readers may be adept enough to start with the databases and directory, the first few resources also contain articles that may be found more explanatory rather than only informative. The featured journals include *ISACA* and *Infosecurity Magazine,* leading sources on news and articles regarding the latest malware, bugs, and outages. The government publication hails from the *Cybersecurity and Infrastructure Security Agency (CISA),* which includes the latest cybersecurity initiatives implemented by the government. The promoted websites and databases are compiled by the *CVE Program, CVE details*, and *NIST,* where the user will find CVE and CVSS data relevant to their threat.

Tips for the Guide:

- Readers are encouraged to conduct further research within the threat landscape of Common Vulnerabilities and Exposures. Adversaries are increasingly innovative and will layer a multitude of attack techniques and vectors to exploit a vulnerability and staying up to date and informed is necessary to be successful within cybersecurity.
- The resources shared below are available at little to no cost; however, certain features require an account or the payment of an access fee. If the resource is behind a paywall, try performing a query of the title within a search engine. Often the resource exists in other contexts.
- Thoroughly read the CVE descriptions and check them against the CVE Glossary Database. Ways to mitigate or eliminate large amounts of known exploits are available at no cost. There is no need to reinvent the wheel when the next vulnerability is waiting to be exploited.

Resources

The Information Systems Audit and Control Association Journal
Source Link: https://www.isaca.org/resources/isaca-journal

Abstract:
ISACA has been a leader within the digital space for over 5 decades. They have worked to advance the standards and resources of the cybersecurity space by offering education, certifications, and a community of industry experts. This journal is considered one of the best cybersecurity publishers as the ISACA organization has over 220 chapters of digital trust professionals worldwide. The resources offered by the ISACA journal are for the majority free to use and access; however, one must be a member to read the exclusive articles and most recent journals. This resource is best targeted towards a cybersecurity professional who would pursue membership within a local ISACA chapter.

The ISACA Journals are published bimonthly and can be accessed in various formats and covers various topics. Some of the more costly yearly reports require an ISACA membership to acquire the material. Recent topics include, enterprise risk, artificial intelligence, resilience and redundance, and the data ecosystem. All highly relevant to risk and threat management. The menu tab also includes a resources tab containing articles that working professionals can reference to their employers when modeling their security framework.

Tips:

- Note that the journals require a membership, the cost is determined by student or professional status. The information contained inside could be dangerous in the wrong hands, it's for the benefit of the cyber world (and ISACA) that the content remains behind a paywall.
- Some of the articles are accessible from other sources or contained in other areas of the website. Try a search engine query to see if your relevant topic is free.
- The search function is configured in a strict manner. When formulating a query be specific and succinct.

The Infosecurity Magazine
Source Link: https://www.infosecurity-magazine.com/

Abstract:
Infosecurity Magazine has been in publication for over a decade. They have continuously provided information and insight to into the field of cybersecurity and have consistently detailed relevant exploits and security incidents. The Infosecurity magazine offers its readers write-ups on current threats, risk management, educational resources, and CVEs that are causing disruption within the cyber world. Their content is offered at little to no cost and is used as a resource by professionals in information security, those who have IT experience, and those who are just beginning.

Useful features curated for users of this magazine include the ability to search Common Vulnerabilities and Exposures by their CVE number, their names, or simply by their description. The website supplies news, topics, features, webinars, white papers, and a directory essential resources and threat reporting agencies. An especially pertinent article that relates to this guide is titled *Navigating the Vulnerability Maze: Understanding CVE, CWE, and CVSS.* The above is a great explanatory resource regarding the application of the concepts mentioned in this guide. Relevant to a recent threat that impacted Windows infrastructures would be the article titled *Windows: New 'BatBadBut' Rust Vulnerability Given Highest Severity Score.*

Tips:

- The most helpful features would include the topics tab and search function. The topics tab will provide recent articles on various security events dependent on a specified sub-topic.
- Sub-topics include Application Security, Cloud Security, Encryption, Risk Management, Malware, etc.
- This magazine often provides information on relevant cybersecurity threats; however, it does not always provide a path to resolution. To manage a specific CVE, check against the CVE database to find a mitigation or patch technique.
- The publications featured here are imperative to staying up to date in the ever-evolving field of cyber security and the CVEs that exist within. Information security professionals are responsible for being cognizant of emerging threats to better protect their systems.

Gov Cybersecurity & Infrastructure Security Agency
Source Link: https://www.cisa.gov/

Abstract:
The Cybersecurity & Infrastructure Agency (CISA) is also known as the United States Coordinator for Critical Infrastructure Security and Resilience. This government organization works to reduce areas of risk surfaces within infrastructures that impact the lives of Americans. Although it is one of the newer federal agencies, being created in 2018, it is an excellent resource for identifying and addressing risk within cyber infrastructures. Being an operational component of the Department of Homeland Security, the materials here can be considered accurate and suitable to the topic.

The website features areas for cyber threats and advisories -current and past, cybersecurity best practices, risk management, training programs, and additional resources. If there is information to be had about mitigating practices surrounding cybersecurity threats, it can be found here. All these items can be located in the menu tab at the top right of the webpage. The search function also resides there. By navigating to Cyber Threats and Advisories through the menu's topics tab the user can view information pertaining to Nation-State Actors, I/D/R/P, Information Sharing, Malware Phishing, and Ransomware, and Securing Networks. The articles in any of the above categories will place users in a better posture to defend their cybersecurity infrastructure.

Tips:

- An especially helpful designation regarding CVEs within the CISA website is the Known Exploited Vulnerabilities Catalog, which is found here: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA includes a physical security tab, a resource not often seen within the other resources shared here. While this isn't detrimental to their functionality and serviceability, the additional facet to CISA makes it one of the best resources included in this guide.

The CVE Program
Source Link: https://www.cve.org/

Abstract:
The CVE Program (maintained by MITRE) serves as a database which users can employ to search and identify known cybersecurity vulnerabilities. This database has been in operation since 1999 and is utilized by most, if not all cybersecurity professionals whether directly or indirectly. Anti-virus programs are often configured to compare malware signatures against established patterns and behaviors that are documented within this database. While not especially helpful against zero-day exploits, the CVE Program helps professionals manufacture a framework for mitigation and treatment.

The CVE records provide professionals with severity scores, version numbers, affected products, additional resources, known patches, mitigation techniques, and CWE information for threat and risk management. The search bar is located at the top-center of the webpage with additional resources and informational snippets located below that. The Resources and Glossary tabs are helpful in providing additional sources of information from all over the web to deciphering any terminology that may be unfamiliar. The website also includes appropriate news articles to the right. An especially helpful article, albeit short, is titled *Vulnerability Data Enrichment for CVE Records: CNA Recognition List, September 23, 2024.* The aforementioned article details CNAs and the CVEs/CVSSs they identify.

Tips:

- This database is straightforward to operate. Users must provide the CVE number in the search box to complete a database query.
- If the CVE number is unknown to the user, the CVE Program provides a hyperlink to the legacy search page on cve.mitre.org wherein users can search utilizing keywords.
- The format of a CVE ID is as follows: (CVE-YYYY-NNNN). It must be fit this form, or the query will not return results.
- If the any of the terms referred to above are not familiar, the CVE Program glossary is found here: https://www.cve.org/ResourcesSupport/Glossary

CVE Details
Source Link https://www.cvedetails.com/browse-by-date.php

Abstract:
CVE Details is an online database powered by the SecurityScorecard that provides a list of CVEs by criteria the user inputs. SecurityScorecard is a cyber risk rating platform. They have integrated specially curated software into solution-based risk evaluations. Their services include digital forensics and incident response, advisory services, penetration testing, and tabletop exercises. This database allows users to sort CVEs by date, type, CVSS scores, EPSS Scores, vulnerable software, attack surfaces, digital footprints, and more. This resource is not completely free, as it offers membership plans. It is incredibly useful when the user is aware of the risk surface of their organizations or adversarial targets.

This website provides a list of years and months for the user to select and view CVEs as well as a list with a certain timeframe (today, yesterday, last 30 days, etc.). Alternatively, the user can use the left side menu to search CVEs using more specific criterion such as known exploits, vendors, emerging CVEs, and open sources vulns, attack surface, vulnerability intelligence, and vulnerable software. The CVE details database uses data directly from the CVE Program with a more user-friendly interface and more extensive search features.

Tips:

- This website can appear visually overwhelming. It's best to start with the CVE search criteria already identified so the sub-categories are serve as informational and secondary to the vulnerability search.
- The information provided is the same information provided by the CVE program; however, it is fed through APIs and within this format it can be easier to locate the vulnerability in question.

National Vulnerability Database (NVD by NIST)
Source Link: https://nvd.nist.gov/vuln-metrics/cvss

Abstract:
The National Vulnerability Database (NVD) is intended to help users generate CVSS (Common Vulnerability Scoring System) assessments dependent on varying metrics that are applicable to an enterprises risk surface. This database also offers a dashboard that has processed over 250 thousand CVE for analysis. The database and dashboard are both produces by the National Institute of Standards and Technology (NIST). This organization came to existence in 1901 to increase the United States ability to remain a technological competitor with the rest of the world. In current day NIST curates tools to enhance science, technology, and the standards involved.

This resource is free and referenced often by cybersecurity professionals. It includes a dashboard that can be accessed via the NVD menu and general tab. This website is simplistic in its design, exploration of the tools is recommended to familiarize the reader with all the components available. Via the NVD menu, the user can explore vulnerabilities, vulnerability metrics, developers, and other resources that the user may find helpful. The Vulnerability Statuses tab is particularly helpful for the user when referencing the status, it's description, and how the statuses interact with each other.

Tips:

- The Common Vulnerability Scoring System bubble will take users to a website out of NIST; however, it would be especially helpful for users who are not familiar with the CVSS scoring factors.
- It is important to note: CVSS is not a measure of risk, but rather a tool for risk management.
- The website includes information on how to cite the dashboard and database towards the bottom of each of their respective pages.