Common Vulnerabilities and Exposures (CVE) List

Task

15m - 35m

Status | Incomplete

Overview of the Exercise

In this exercise you will learn about the MITRE common vulnerabilities and exposures (CVE) list, what it contains, and how you can use it to learn about vulnerabilities. You will then search for a vulnerability in three different items of your choosing and create a brief write-up of what you are able to learn.

> **Reflection Question**
>
> Is the CVE list intended to replace all other vulnerability databases?

About the CVE

The MITRE organization hosts the CVE list, which aims to identify, catalogue, and describe as many exploitable vulnerabilities as possible. The program is publicly available, and contributions come from global partner organizations. The program and list helps to bring consistency about how vulnerabilities are labelled and identified across the industry and the globe.

Exercise

Prepare

1. Explore the general materials about the CVE program to become familiar with the history of the program, and other programs linked to the CVE. Make notes about elements you think are important to review and reference.
2. Dive into the details of the CVE records. Make notes about:

- The types of information documented in each CVE record about a vulnerability
- The process to get a vulnerability recorded in the CVE list, including information that must, should, and may be included in the record

1. Review the CVE List Search Tips page for guidelines on how to search the CVE list for vulnerabilities related to a particular product. Make notes as you see fit.

Practice

> For this exercise, you might want to reach out to a colleague or two and work together.
>
> Working together generates a wider variety of ideas, and also mimics how you might complete this kind of task in a work setting.

Choose three different products that you want to search on the CVE. Try to include items from three different categories for a wider variety of practice (e.g., IoT devices, network devices, types of software, computers, mobile devices, etc.)

For each product, find at least one vulnerability in the CVE list and create a brief write-up that answers the following questions:

- What is the vulnerability?
- Has the vulnerability been repaired or patched?
- How severe of a concern was the vulnerability? Would it affect just a small part of a business or would it potentially be devastating to the organization as a whole? How do you know and how did you make that determination?

Reflect

Consider the practical use of the CVE list as a professional tool. Address these points in your write-up:

- Where did you have to go to find a full description of what each vulnerability did or allowed?
- Where did you find out how to fix it or mitigate it?
- How did you find additional information about a vulnerability, such as threat rating and remediation recommendations?
- Suggest at least two reasons why, as a Cyber Security professional, it is important for you to be aware of databases like the CVE and how to use and understand them.

Participate

1. If you want, you can share your group's write-up on Discord.
2. Give feedback to write-ups from other groups; remember to keep feedback and comments positive and constructive.
3. Try to vary who you give feedback to, so every group can get some feedback.
4. Read the feedback on your own write-up and note any useful comments or questions from your peers.

Conclusion

By the end of this exercise, you should be familiar with the CVE list, what it is for, and how to effectively navigate it to find vulnerabilities related to a given product. You will have reflected on the importance of the CVE list for Cyber Security professionals and developed skills to help you use it in future scenarios.

Next, you will explore how to score vulnerabilities and customize that score to your specific needs.

Previous
Vulnerability Concepts

Next
Vulnerability Severity

W05D2

Tue Jul 23

- Outline & Notes (1)
- Lectures (1)
- Work (10)

  10 hrs

  - Project: Risk Management Case Study
  - Risk Management Case Study Presentation ✓
  - Regulatory Drivers & Cyber Security Compliance
  - Cyber Security Regulations Presentation
  - Course Reflection ✓
  - Overview - Vulnerability Assessment
  - Vulnerability Concepts
  - Common Vulnerabilities and Exploits (CVE) List
  - Vulnerability Severity
  - Security Vulnerabilities Scenarios with AI
- Other (1)

W05D2 Schedule »