Necessary Skills Now

STUDENT: PRODUCT ANALYSIS

Document Version: 2018-10-01

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Contents

Overview

This project includes the following tasks:

1. Gather product information
2. Analyze and differentiate product vulnerabilities
3. Recommendation based on empirical data collection

Objective: Product Selection Recommendation

Organizations depend on cybersecurity professionals to evaluate technologies and products. Organizations may use the analysis to make purchasing recommendations or to establish equipment and deployment standards. Product analysis is a workplace skill that is universal throughout the business community. Evaluating technologies and products helps to ensure that the workplace environment remains secure.

As stated in the NIST Special Publication 800-36, product selection involves people throughout various departments within the organization. Each person involved in the product selection process must understand the importance of security.

In evaluating various products and technologies, the organization analyzes identified threats and vulnerabilities as part of the selection process.

Common Vulnerabilities and Exposures (CVE) provides common names (also called CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVEs provide reference points so that information security products and services have a common baseline for evaluation. CVEs make it easier to share data about tools, repositories, and services.

The CVE Details website allows individuals to perform a deep analysis in comparing technologies.

When selecting products and technologies, the organization's team needs to consider the threat environment and the security functions to lessen the risks to an acceptable level.

Website Links

NIST Guide to Selecting Information Technology Security Products

Common Vulnerabilities and Exposures

CVE Details

Project Scenario

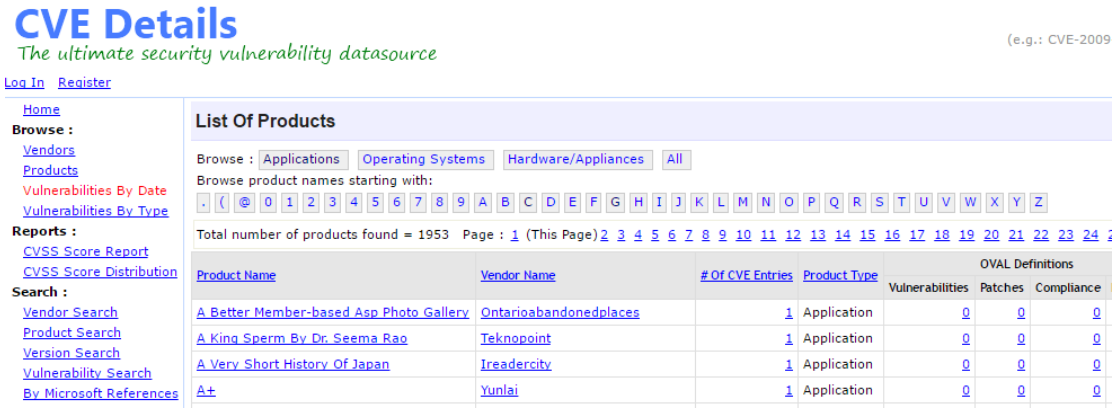
Acme Corporation has recently experienced cyber-attacks and data breaches that have resulted in a significant financial loss and a loss of consumer confidence. Acme hired a new chief information security officer. The CISO informed the cybersecurity staff that the organization would undergo a comprehensive threat analysis and begin to collect data to establish purchasing and deployment standards. The CISO wants to ensure that the organization uses empirical data in selecting products and establishing of standards in lieu of opinions of staff members or a sales pitch from vendors.

Over the last decade, the federal government and other organizations collected substantial data regarding product vulnerabilities and flaws. This data is freely available to organizations interested in performing product analysis. The Common Vulnerability Exploit (CVE) database is one example of a national resource available to cybersecurity professionals used to perform product analysis. The CVE Details website allows individuals to perform a deep analysis in comparing technologies.

After several incident response investigations, it is apparent that many attacks were the result of browser and email vulnerabilities. The CISO has tasked the cybersecurity staff with analyzing the organization's Internet browsers. The investigations identified that over 95% of all users employ one of four browsers: Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Microsoft Edge.

1 Gather Product Information

1. Refer to the resources at NIST Guide to Selecting Information Technology Security Products (see Roles and Responsibilities, pp 4-5) and Common Vulnerabilities and Exposures (see About CVE) sites.
2. Work in your assigned teams to use the CVE Details website to collect and analyze vulnerability-related information for the four browsers used at Acme Corporation.



   a. Select **Browse > Products** from the menu in the left column.
   b. Click **Applications** from the List of Products.
   c. Select the appropriate character, number, or letter.
3. The analysis should include the number, types, and the criticality of the vulnerabilities for each of the three browsers.
4. Organize the results found into tables and charts using Microsoft Excel.

2 Analyze and Differentiate Product Vulnerabilities

1. Using the team's research data, identify strengths and weaknesses of each product.
2. Identify the features and tools embedded in the products, which mitigate vulnerabilities.
3. Evaluate the ability that each product has for monitoring potential attacks and controlling potential vulnerabilities.
4. Generate a two-page report summarizing the team's findings.

3 Recommendation

1. Make a recommendation for the browser(s) that Acme Corporation should use.
2. Support the team recommendation with data from the analysis.
3. Identify the benefits and challenges of implementing the team's recommendation.
4. Prepare a PowerPoint presentation for the CISO and all department heads to present the team's results.

Conclusion

The CVE Details website is the web interface to CVE vulnerability data. CVE is available to the public and is a compilation of known information security vulnerabilities and exposures.