The Economics of Cybersecurity: Homework 4

Due: February 13 at **5:00pm**

CVE Exploration (10 points)

One of the main objectives in this class is to examine the various attempts that have been made to mesaure and quantify security. One notable example of this is the National Vulnerability Database (NVD) and associated list of Common Vulnerabilities and Exposures (CVEs).

All CVEs follow the same naming convetion: The tag "CVE", folllowed by the year of discovery, and then by a chronological index number (e.g. "CVE-2024-22211"). The Cybersecurity and Infrastructure Security Agency (part of the U.S. Department of Homeland Security) maintains a database of CVEs. Browse the list of known exploited vulnerabilities on CISA's website: https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Choose and click on a CVE from the list and answer the following questions:

1. What your chosen CVE's ID?

2. What software is affected by this vulnerability?

3. What is the Base Score of your chose CVE?

4. Look under "References to Advisories, Solutions, and Tools", where there may be a link to an advisory from the software vendor. Can you determine if this vulnerability has been patched? Can you find a link to the patch itself?

5. Although each CVE is unique, many have the same underlying root causes. Hence CVEs are taxonomized using the Common Weakness Enumeration (or CWE) list. What is this CVE's CWE ID and Name? Look under the "Weakness Enumeration" section. Click on the CWE link and briefly describe what the weakness is.

The "Base Score" above is a quantitative indicator of the CVE's severity. CVEs are given a severity score using the Common Vulnerability Scoring System (CVSS), which is a series of calculations based on metrics like exploitability and impact. Take a look at the scoring calculator here:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

6. Select various metrics and see how they affect the scores. Which combination of metrics yields the highest possible score of 10? This should be fairly easy to do, but you may also click on "Show Equations" to observe exactly how scores are calculated.

Paper 1 (0 points)

Read the paper A Large-Scale Empirical Study of Security Patches. Come to class prepared to discuss the paper (you may be called upon at random in class).

Paper 2 (0 points)

Read the paper How Much is Performance Worth to Users?. Come to class prepared to discuss the paper (you may be called upon at random in class).