COIT20246 Networking and Cyber Security

Week 08 Tutorial Activities

Attacks and Vulnerabilities

Aim to complete Tasks 1 to 3 during the tutorial, and have all tasks completed before your next tutorial.

# Task 1. CIA Protections

For your Project, create a list of the important assets in the network, especially data and equipment. Then use the CIA Triad to identify what you want to protect and why. For example, you may identify the “security cameras” as an important asset, in which case you may say:

* *Asset 1*: security cameras o *Protection*: availability
  + *Reason*: if the cameras are down, then no recordings will be available if a crime is committed

Or you may identify the names and personal details of tenants (those renting) stored on a local server as important:

* *Asset 2*: tenant personal details o *Protection*: confidentiality
  + *Reason*: a tenant should not be able to see the personal details of other tenants

Try to identify multiple assets, and consider the different CIA protections on each, e.g. is the integrity protection important for Asset 2?

There is no set number of assets to consider. Feel free to discuss with other students in your class. The assets you list will be helpful for your tutorial and project next week.

In your journal:

* List the assets, and for each asset, give the protection and reason.
* *Asset 1: Network Devices*
  + *Protection: Availability*
  + *Reason*: the network devices should be available for the business to carry out all their necessary business operations
* *Asset 2: Network Traffic*
  + *Protection: Integrity*
  + *Reason:* The network traffic is sent out by the organization to perform various activities and without integrity verification, these network traffic may not be accepted by destination server.
* *Asset 3: Personal information*
  + *Protection: Confidentiality*
  + *Reason:* These information regarding customers and employees may lead to identity theft as such, they need to be protected.

# Task 2. Threat Sources and Motivation

For your Project, create a list of the most likely types of adversarial threat sources (attackers), and their motivation. For example:

* *Threat Source 1*: Neighbour o *Motivation*: wants to get free Internet access
* *Threat Source 2*: Competitor real estate agency o *Motivation*: …

In your journal:

* List the threat sources, and for each threat source, give the motivation.
* *Threat Source 1:* DDoS attacks
  + *Motivation*: wants to disable the website for certain period of time
* *Threats Source 2:* Adversaries
  + *Motivation:* Wants to steal information and data of the company using malwares that damage the company
* *Threats Source 3:* Hackers
  + *Motivation:* Perform session hijacking attack to gain unauthorized access to the network.

# Task 3. Explore Vulnerabilities

Using NIST NVD, explore CVEs over the past 12 months, and select three different CVEs, one with Critical security, one with High severity and one with Medium severity. You either randomly explore several CVEs from the full listing ([https://nvd.nist.gov/vuln/full-listing)](https://nvd.nist.gov/vuln/full-listing) or search for CVEs

[(https://nvd.nist.gov/vuln/search)](https://nvd.nist.gov/vuln/search). Try to find CVEs from companies or software/hardware that you are

Attacks and Vulnerabilities 1 COIT20246 Networking and Cyber Security

familiar with, and for vulnerabilities that you can understand (at least partially). That is, you may need to read 5-10 CVEs before you select your chosen three CVEs to report on.

For the three selected CVEs, identify the following: CVE ID; CVE Description; Date; CVSS Version 3 Score; impact on Confidentiality, Integrity and Availability; at least one CWE (ID and Name); company; description of the product affected (name and what it is for); simple explanation of the vulnerability; detection and/or mitigation techniques.

Most of the above information can be found from the CVE entry on NVD, except the following:

* For the impact on CIA, click on the Base Score; it will take you to a page which is the CVSS Calculate for the CVE, and you will find the CIA impact under Impact Metrics.



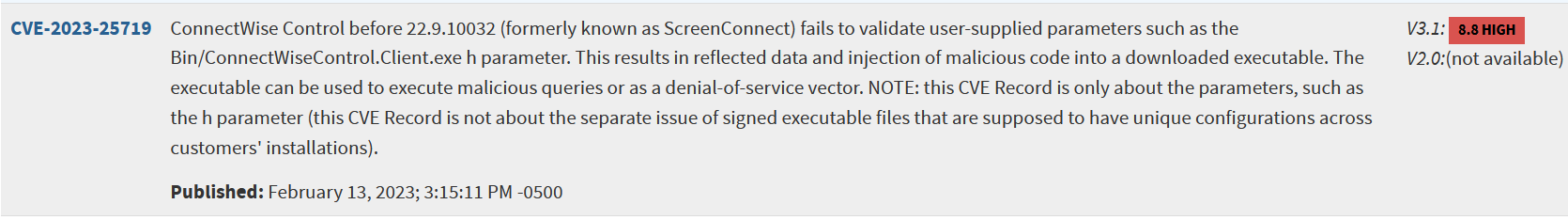
* For the company name, product description and detection/mitigation, you may follow the links to the vendor advisory and read more details.
* For the simple explanation, you should write in your own words, based on reading: the CVE, the CWE and the vendor advisory. (Hint: the CWE description is often the easiest to read).

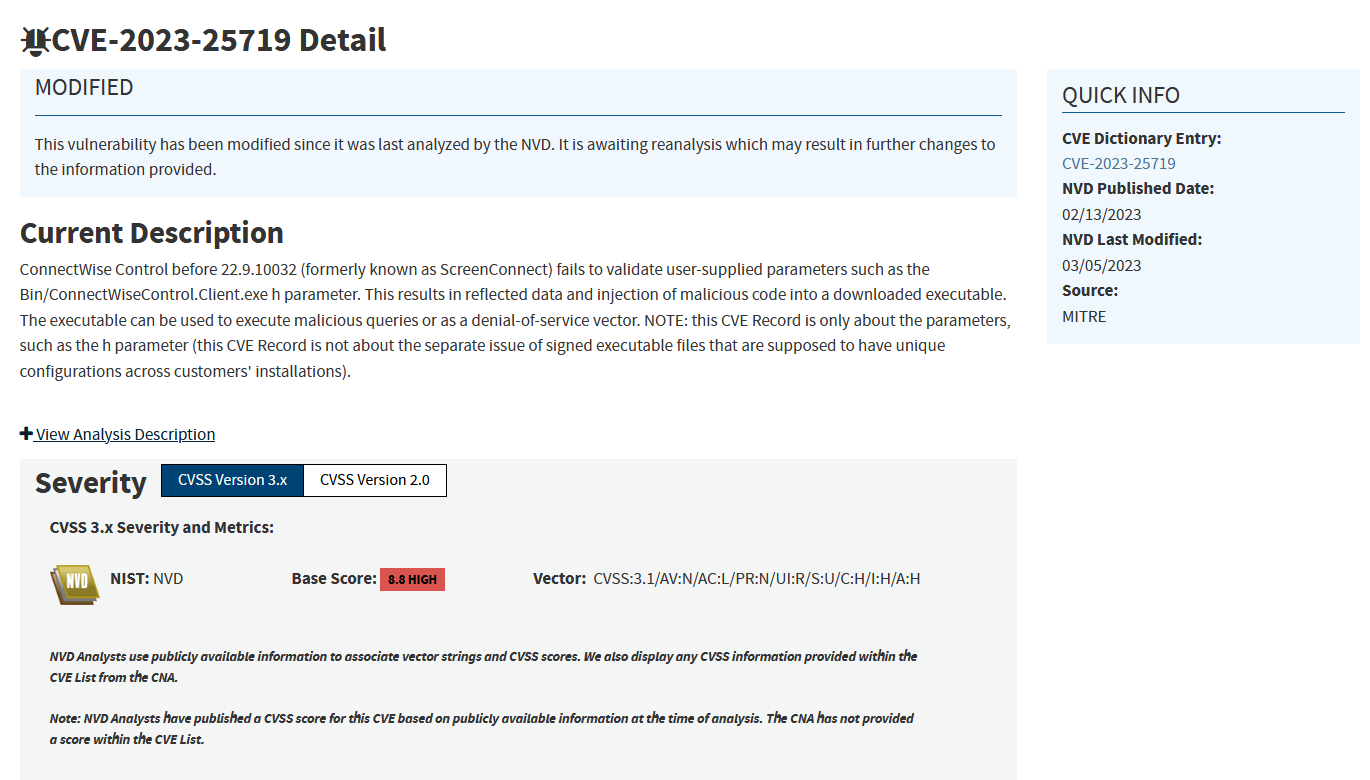
In your journal:

• Include the details for the critical, high and medium CVE.

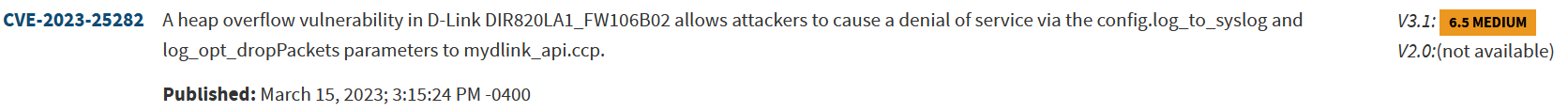
The list of CVEs is as follow:

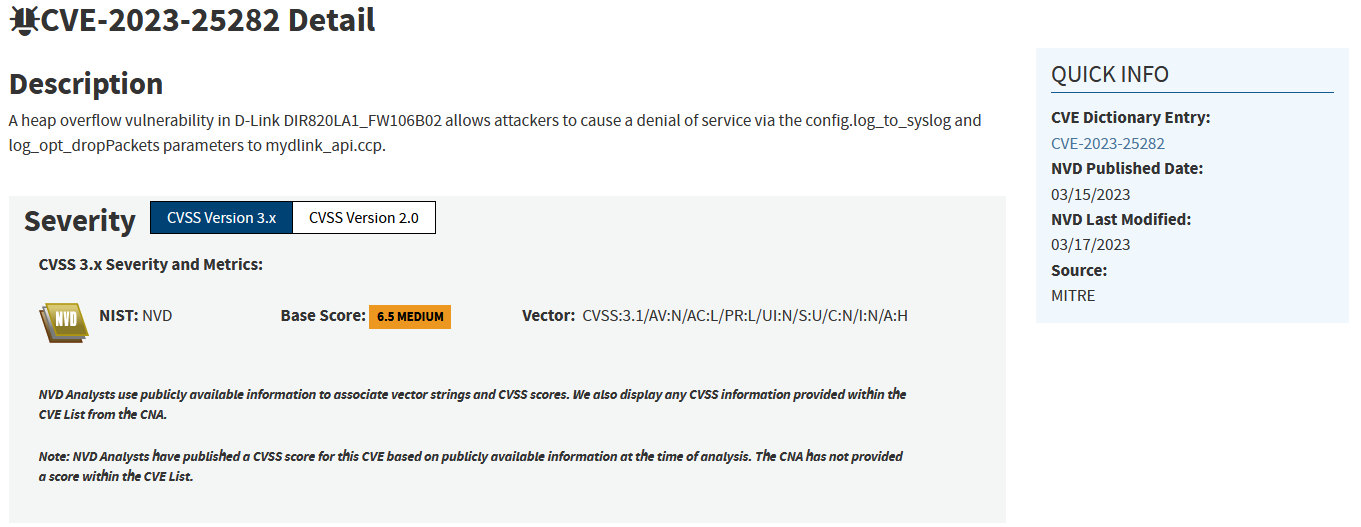
* CVE-2023-25719 with 8.8 High severity



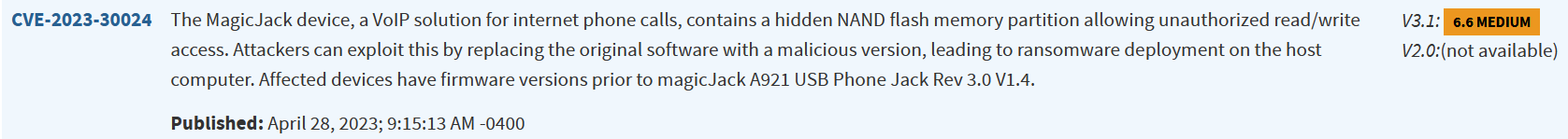


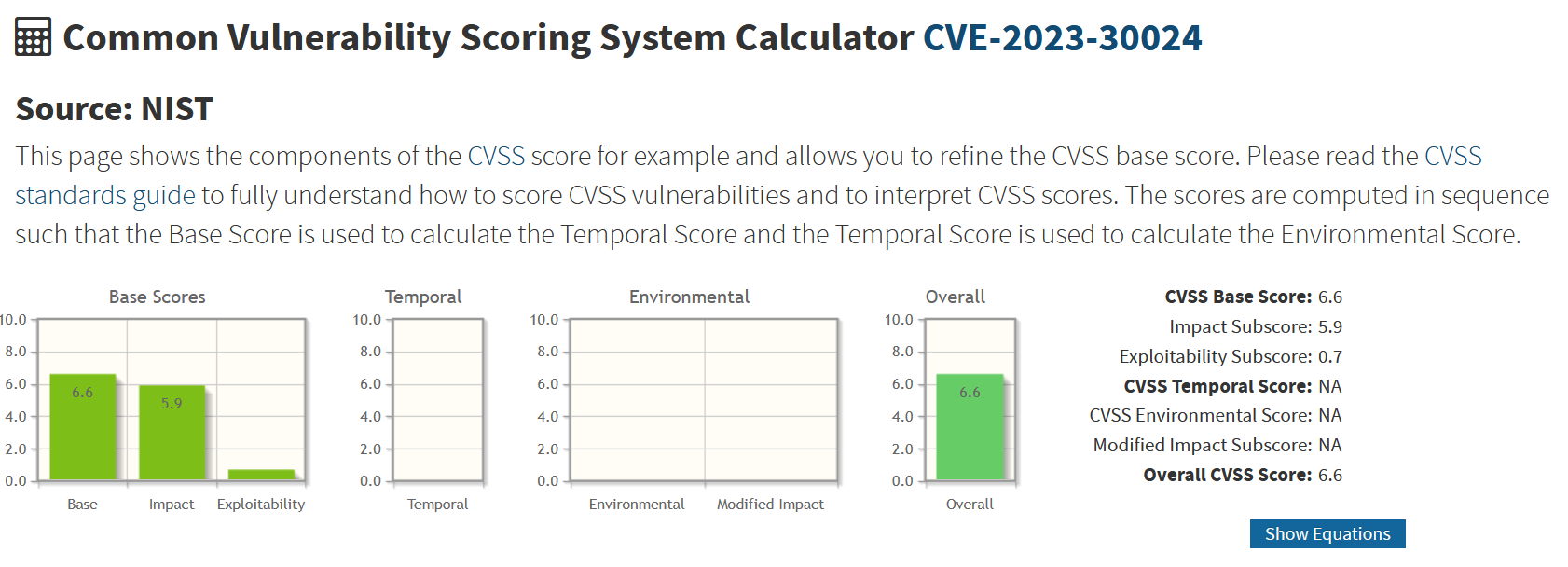
* CVE-2023-25282 with 6.5 Medium severity



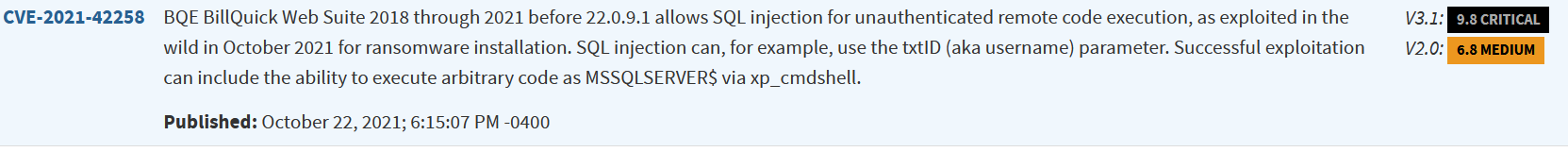


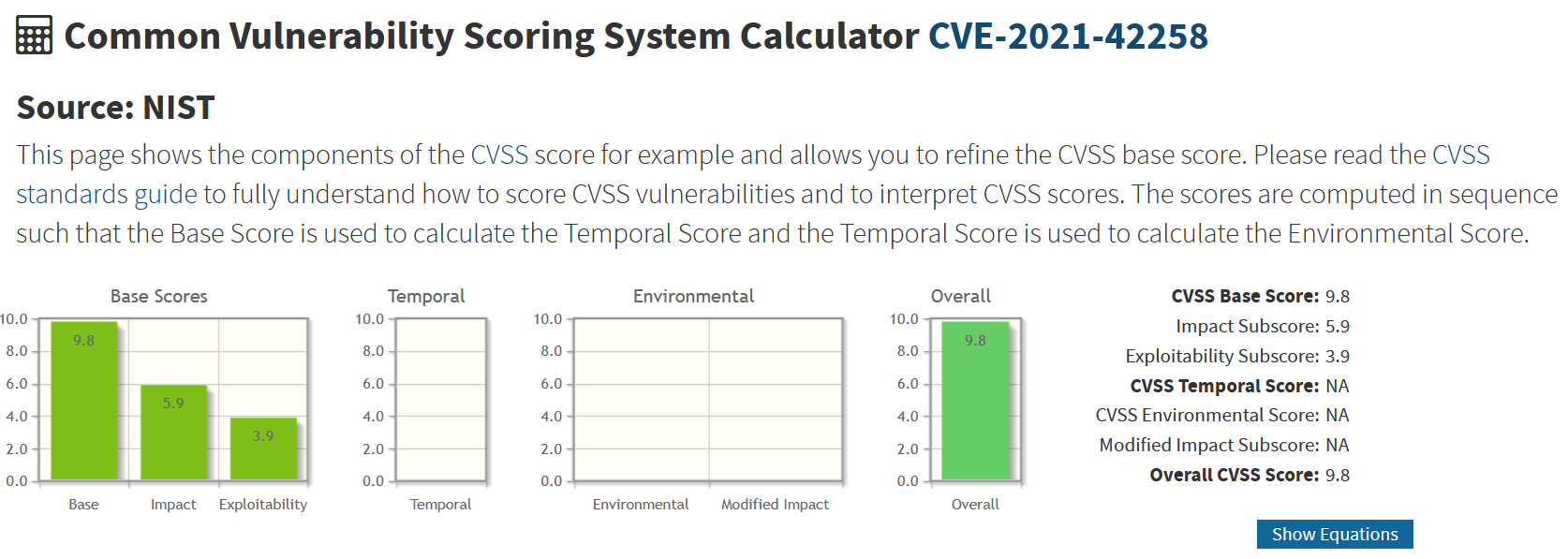
* CVE-2023-30024 with 6.6 Medium severity



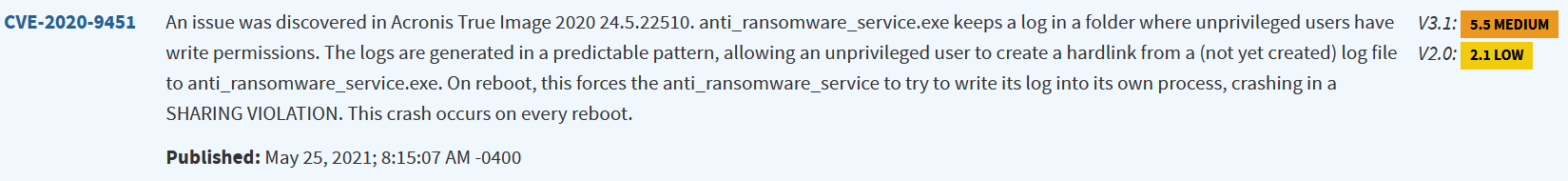


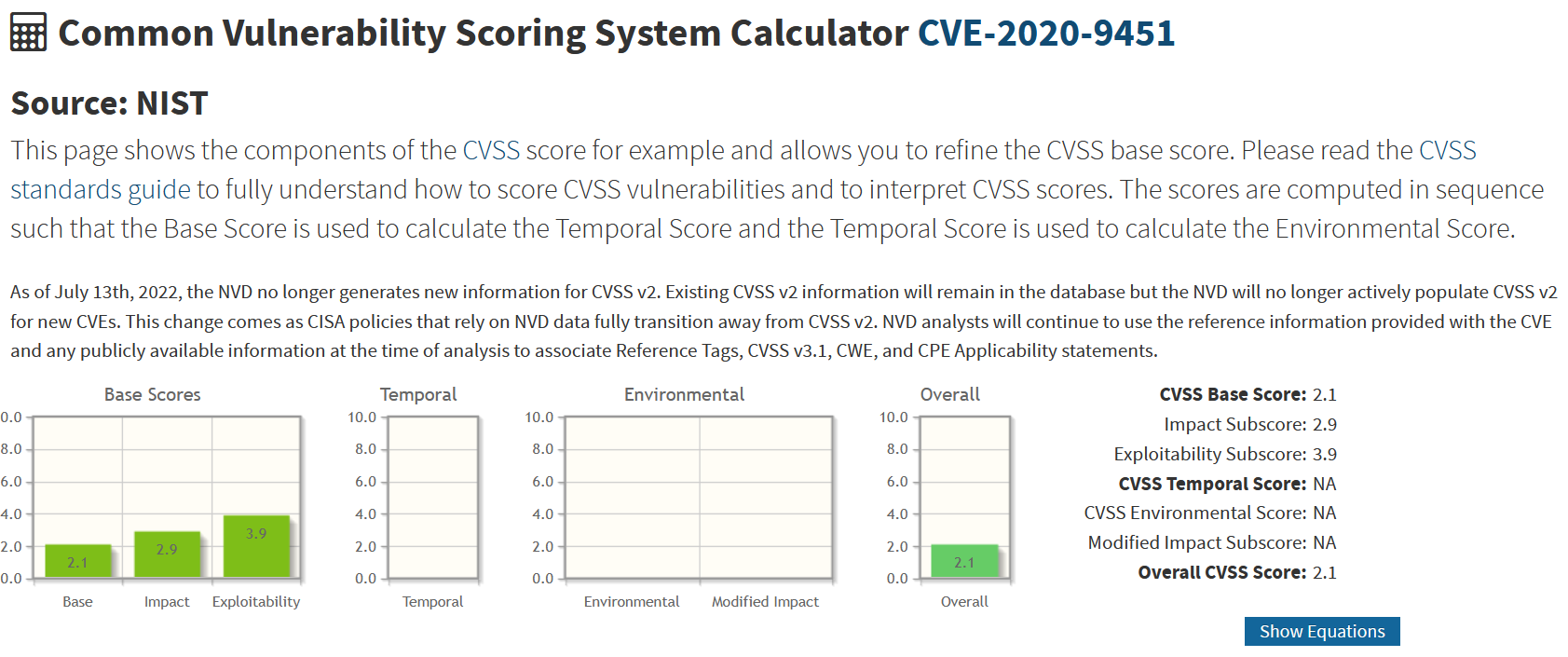
* CVE-2021-42258 with 9.8 Critical severity



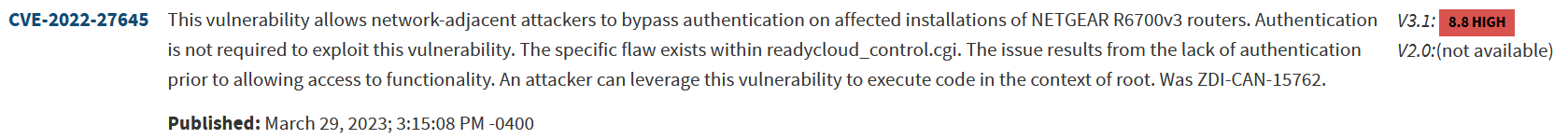


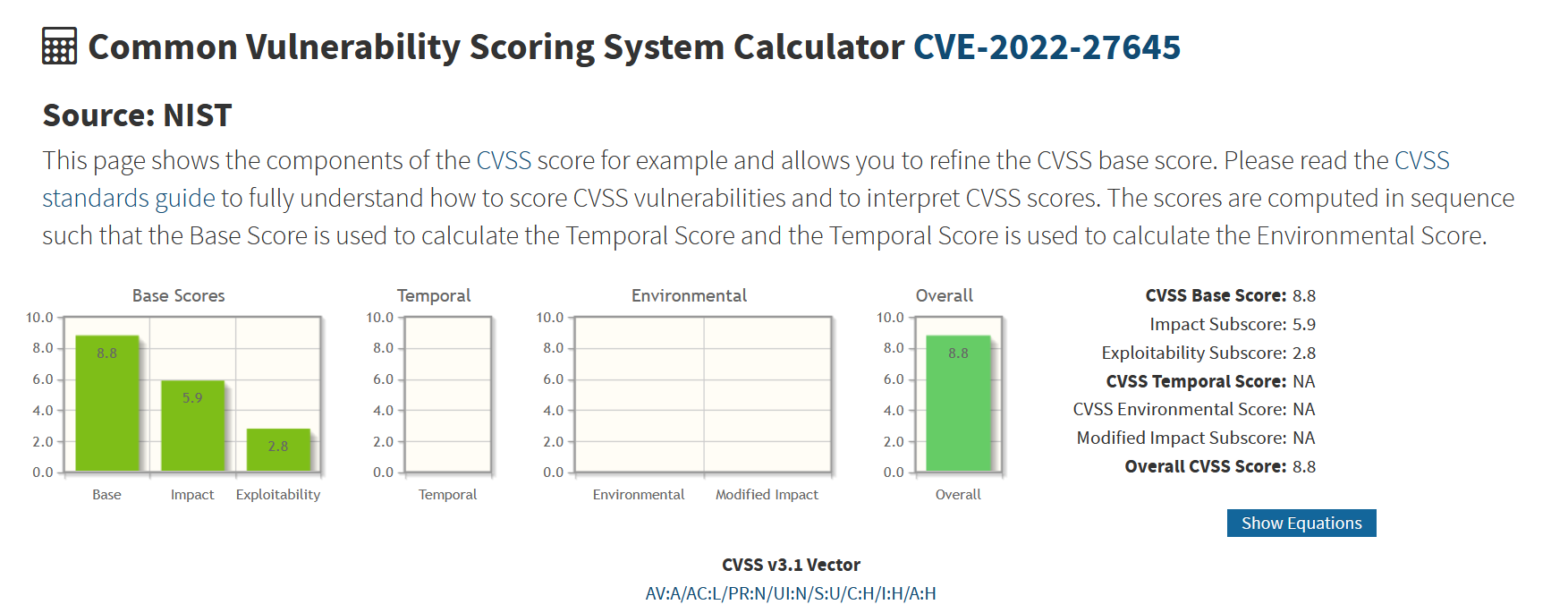
* CVE-2020-9451 with 2.1 Low Severity





* CVE-2022-27645 with 8.8 high severity





# Task 4. Vulnerability Disclosures

CVEs are normally created when reported to MITRE by product vendors (e.g., the company that makes the software or hardware). The vendors may learn of the vulnerability in different ways; however a common approach is that security researchers discover the vulnerability and report it direct to the vendor. Consider the time from when a security researcher reports the vulnerability to the vendor (done privately), until when the vendor reports the vulnerability to MITRE (creating a CVE and making it public). Why might a vendor take time before making the vulnerability public? What is a reasonable time? If the vendor does not make the vulnerability public within a reasonable time, should the security researcher make it public without the vendors permission? Consider these and other issues regarding disclosure of vulnerabilities, preferably discussing in class. Also read about responsible/coordinated vulnerability disclosure and bug bounty programs, e.g.

* <https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html>
* <https://www.microsoft.com/en-us/msrc/cvd>
* <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330>
* <https://www.broadcom.com/support/security-center/vulnerability-management>• <https://cve.mitre.org/cve/researcher_reservation_guidelines>

A vendor might take their time for Vulnerability disclosure because a vulnerability will imply that the service or application that they have provided have weaknesses in them which might put the customers at risk and so, the vendor will have to assess the damages that the vulnerability might cause and find a solution for it before disclosure which is why a vendor might take their time. A reasonable time would be a week or so. If the vulnerability is too high and puts a lot of people and information at risk and the vendor is not doing anything about it then yes, the security researcher should make it public without vendors’ permissions but doing so may put his/her opportunities at risk in the future.

In your journal:

* Write up your own viewpoint that discusses the issues with vulnerability disclosure.

While vulnerability disclosure is potentially damaging ones’ reputation as vendor, it is also necessary to provide as much visibility as possible to the customers to maintain customers’ trust. The issues with vulnerability disclosure are that the customers that are using the product will stop using and the vendor themselves should encourage them to do so in order to maintain keep the customers ensured but when they do that, they will have incurred various financial damage. This is why the vendor must solve the vulnerability issues and provide a security patch as soon as possible and if needed, CVE can be used to ensure security by minimizing the vulnerability.

Attacks and Vulnerabilities 2 