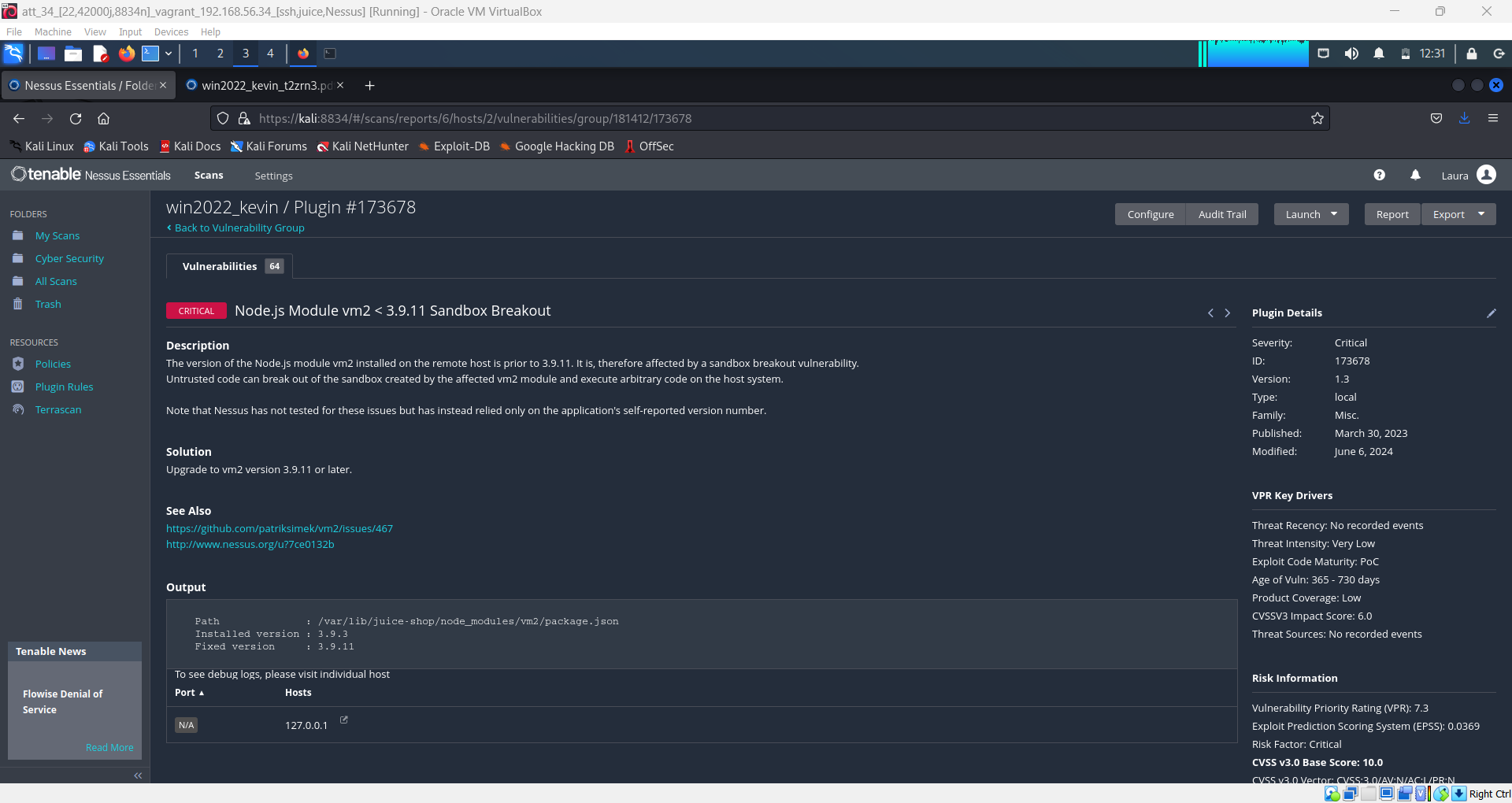
**Week 8 Portfolio**

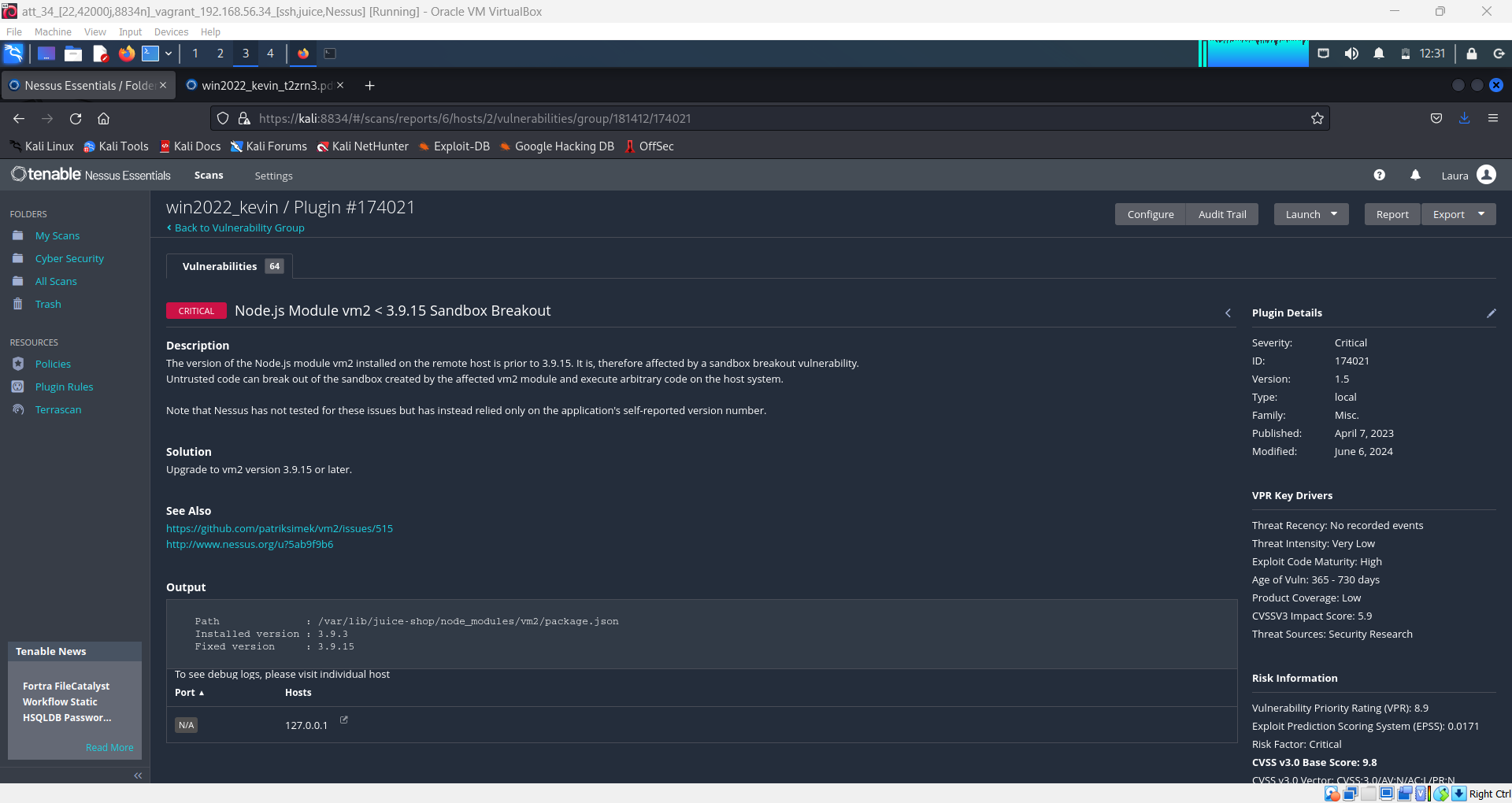
The following steps were followed to prioritise vulnerabilities in our information system:

1. We identified three critical CVEs from the Nessus report CVE-2022-36067, CVE-2023-29017, and CVE-2024-0985. Each of these vulnerabilities was chosen based on their severity, exploitability, and relevance to the information system's environment. Here are three CVEs identified from our Nessus report:

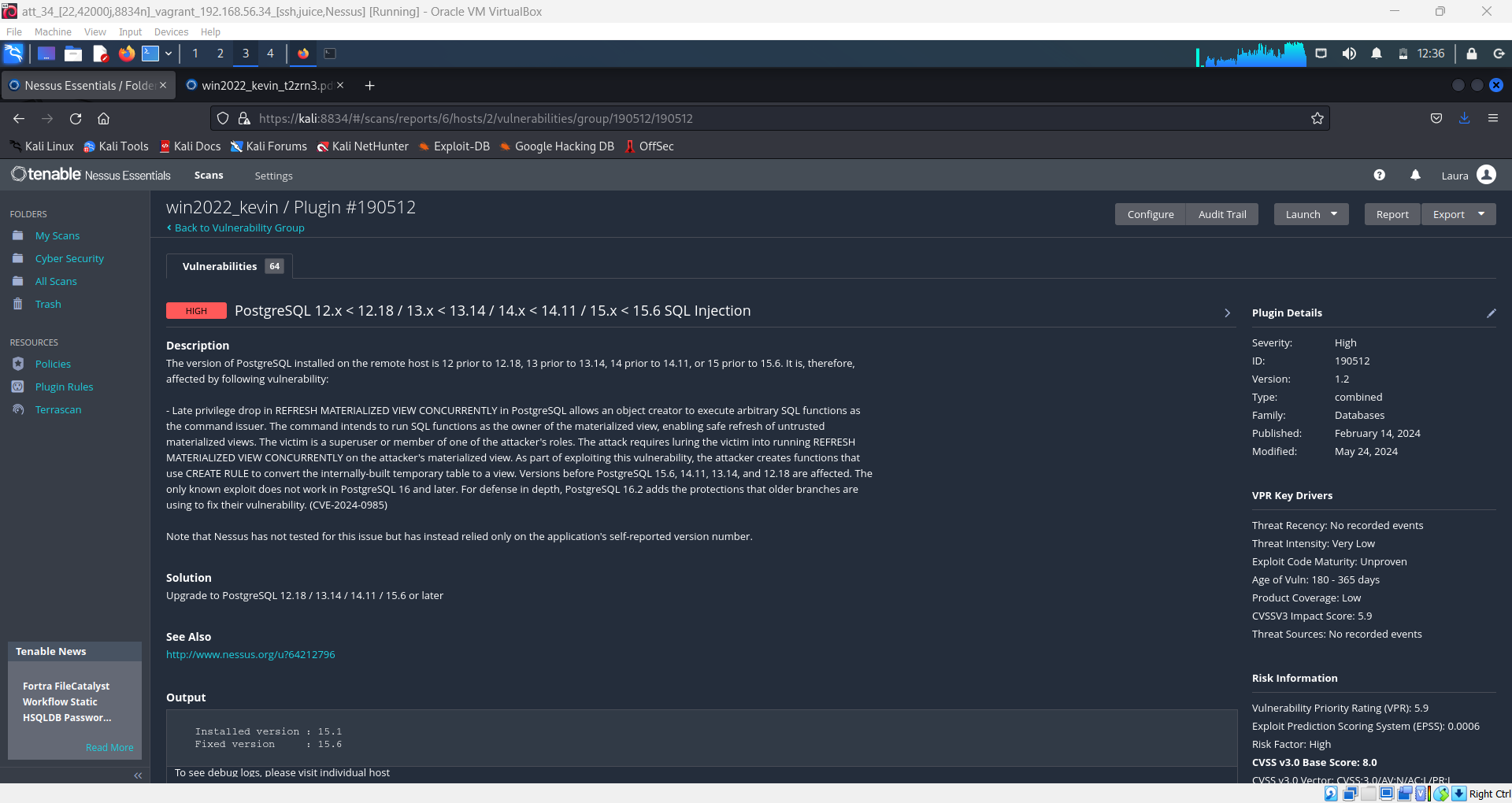
* CVE-2022-36067 (Node.js Module vm2 < 3.9.11 Sandbox Breakout)



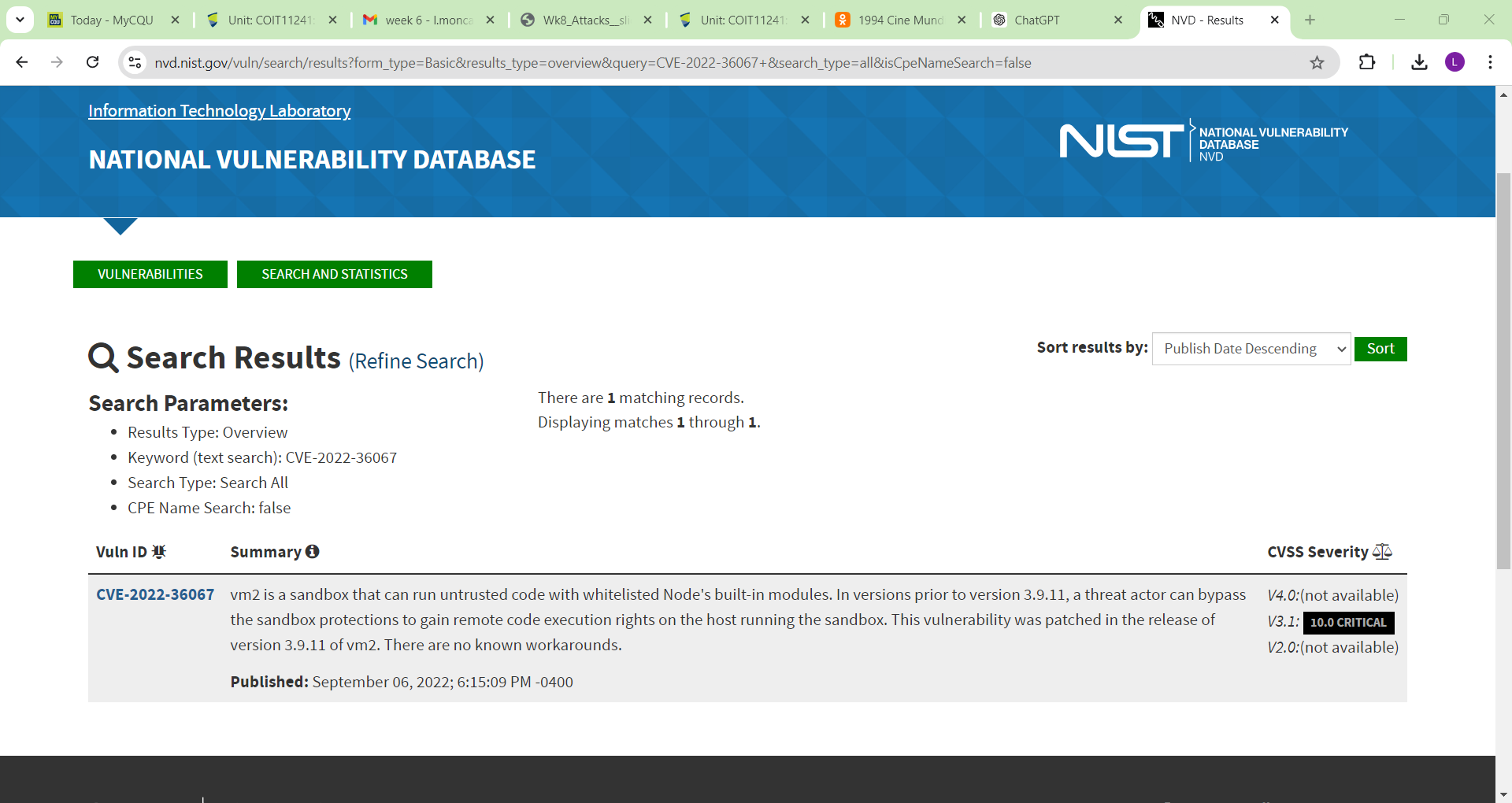
* CVE-2023-29017 (Node.js Module vm2 < 3.9.15 Sandbox Breakout)

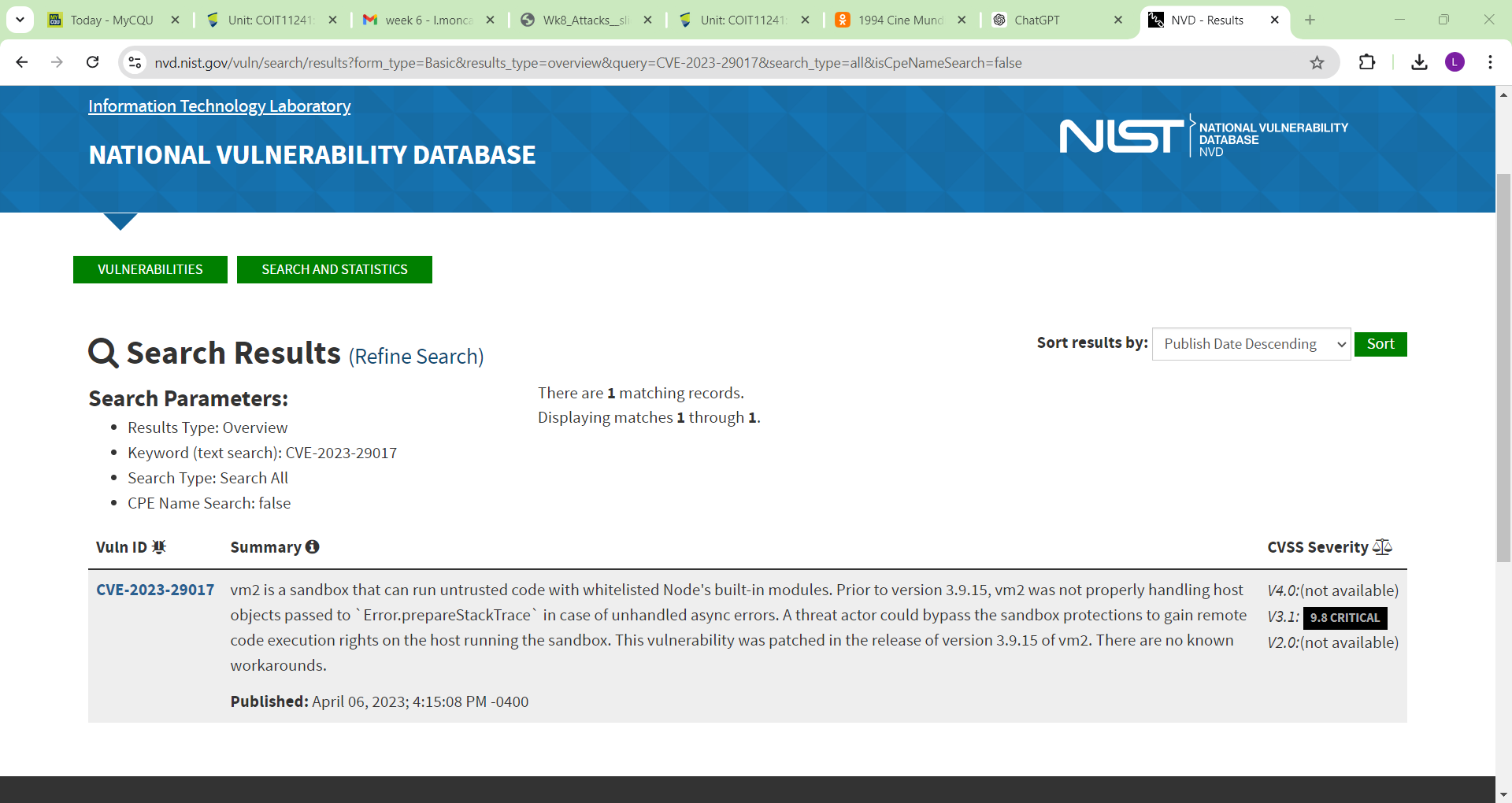


* CVE-2024-0985 (PostgreSQL SQL Injection)

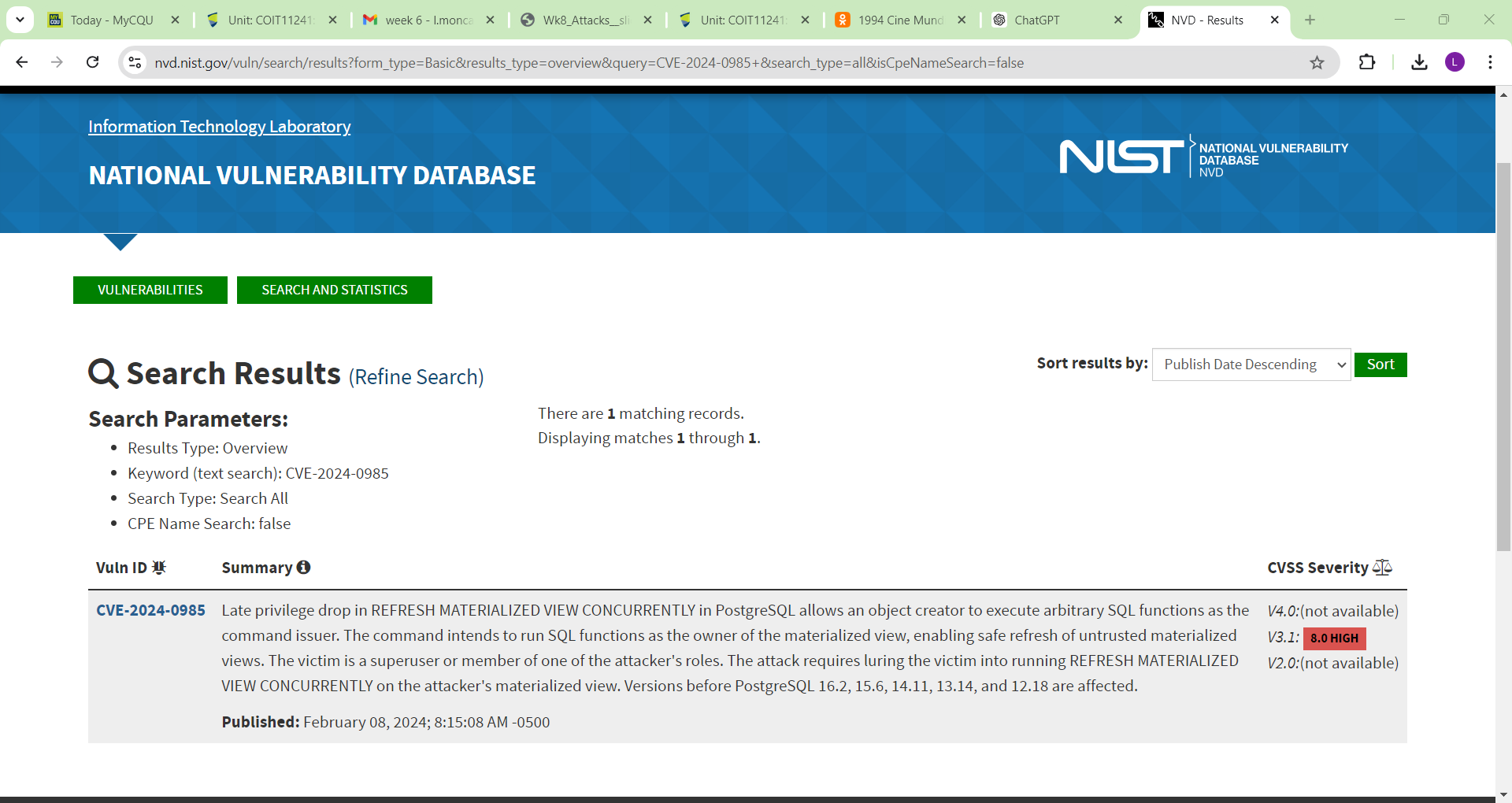


1. For each CVE, we examined the Common Weakness Enumeration (CWE) associated with the vulnerability. For example:
   * CVE-2022-36067 and CVE-2023-29017 are both linked to CWE-693 (Protection Mechanism Failure), which involves weaknesses that lead to the failure of critical security mechanisms.





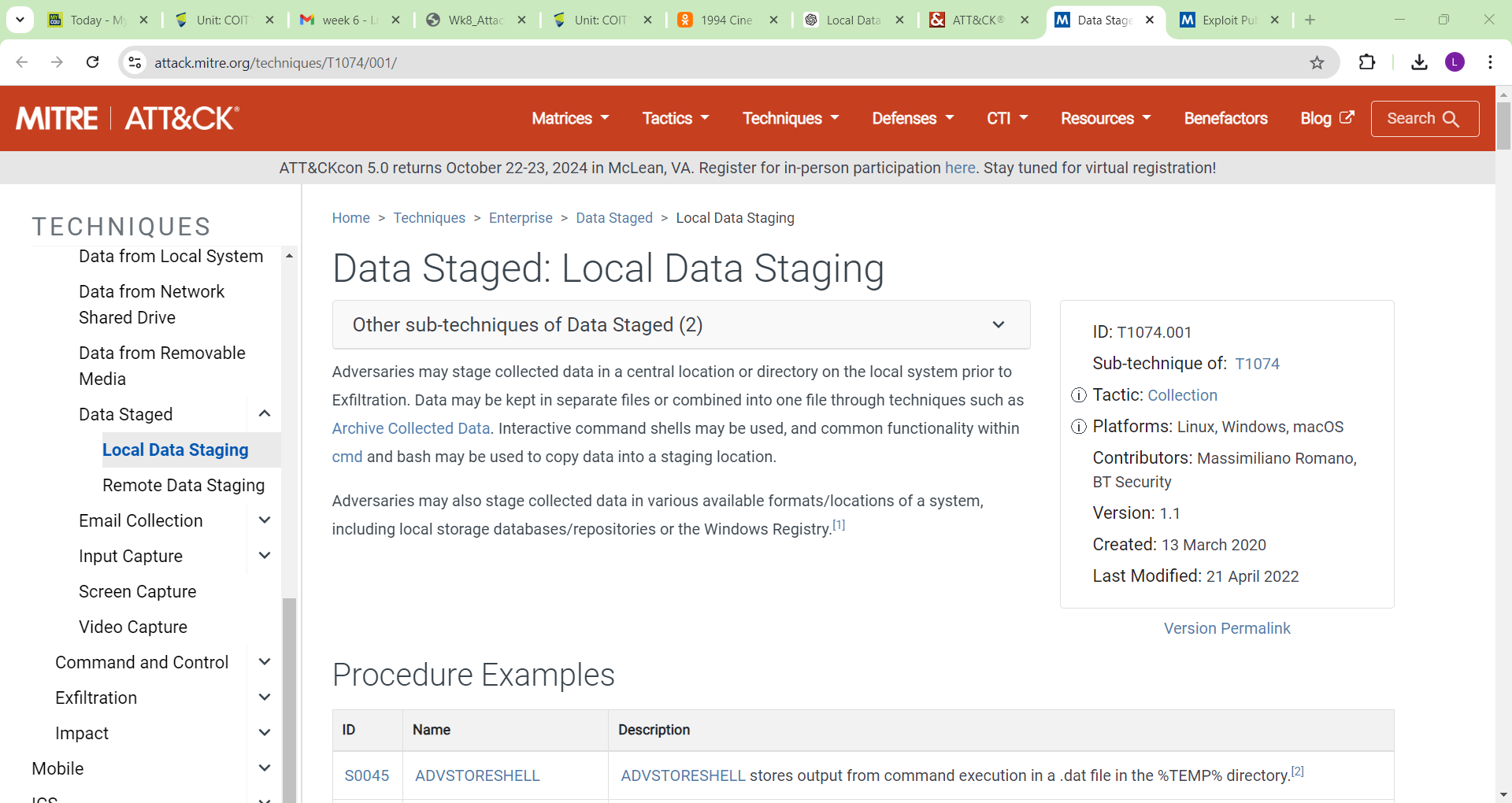
* + CVE-2024-0985 is mapped to CWE-89 (SQL Injection), a common and severe weakness that can lead to unauthorised access or data manipulation.



1. Using the Common Attack Pattern Enumeration and Classification (CAPEC), we identified the specific attack patterns related to each CVE:

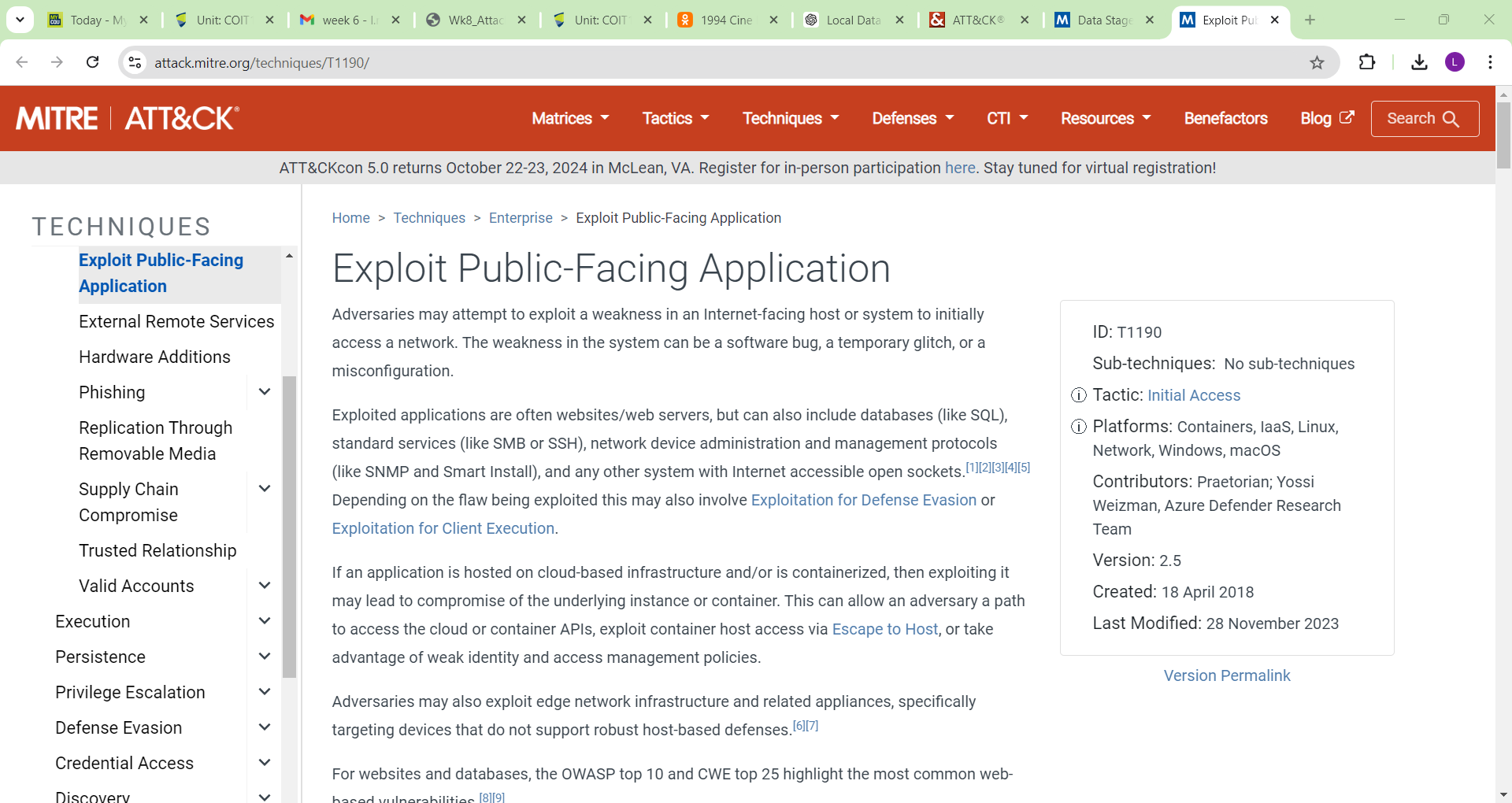
* CVE-2022-36067 and CVE-2023-29017 are linked to CAPEC-111 (Sandbox Escape), which describes techniques used to break out of a restricted execution environment, often to gain higher privileges.
* CVE-2022-36067 and CVE-2023-29017 were associated with T1074.001 (Local File Manipulation), which involves adversaries exploiting local files for privilege escalation or post-exploitation.

<https://attack.mitre.org/techniques/T1074/001/>



* CVE-2024-0985 relates to CAPEC-66 (SQL Injection), an attack that involves injecting malicious SQL code into an application to manipulate its database.
* CVE-2024-0985 was linked to T1190 (Exploit Public-Facing Application), where adversaries target vulnerabilities in public-facing services or applications to gain initial access.

<https://attack.mitre.org/techniques/T1190/>



1. We researched whether these techniques were commonly used by the BumbleBee malware or similar threat actors:

* Both CVE-2022-36067 and CVE-2023-29017 involve sandbox escapes, which are relevant to BumbleBee's post-compromise activities. Threat actors, including BumbleBee, frequently use similar techniques to elevate privileges.
* CVE-2024-0985 is a classic SQL injection attack, a method often utilized in reconnaissance and initial access phases. BumbleBee is known for phishing campaigns that exploit public-facing vulnerabilities (T1190), making this a potential vector for initial access.

1. After gathering and analysing this information, we organised it into a structured format, filling in the CWE, CAPEC, ATT&CK, and Used by Threat Actor columns. This helped illustrate the connection between each CVE and how it could be exploited by BumbleBee or similar threat actors.

**CVE-2022-36067**

|  |  |  |  |
| --- | --- | --- | --- |
| **CWE** | **CAPEC** | **ATT&CK** | **Used by Threat Actor** |
| CWE-693 | CAPEC-111 (Sandbox Escape) | T1074.001 (Local File Manipulation) | Yes, similar techniques used for privilege escalation or exploitation |

**CVE-2023-29017**

|  |  |  |  |
| --- | --- | --- | --- |
| **CWE** | **CAPEC** | **ATT&CK** | **Used by Threat Actor** |
| CWE-693 | CAPEC-111 (Sandbox Escape) | T1074.001 (Local File Manipulation) | Yes, aligns with post-compromise techniques like sandbox escapes |

**CVE-2024-0985**

|  |  |  |  |
| --- | --- | --- | --- |
| **CWE** | **CAPEC** | **ATT&CK** | **Used by Threat Actor** |
| CWE-89 | CAPEC-66 (SQL Injection) | T1190 (Exploit Public-Facing Application) | Yes, aligns with BumbleBee’s reconnaissance and phishing methods |

* **CVE-2022-36067 and CVE-2023-29017:** Both relate to sandbox breakout vulnerabilities (CWE-693, CAPEC-111). These vulnerabilities can be mapped to the ATT&CK technique T1074.001, used for local file manipulation, which is a typical step post-exploitation by threat actors, including BumbleBee.
* **CVE-2024-0985:** This is a SQL injection vulnerability (CWE-89, CAPEC-66). It maps to T1190, which covers exploitation of public-facing applications, a common tactic for threat actors like BumbleBee to gain initial access.

1. Based on the analysis of exploitability and threat actor behaviours, I concluded whether each CVE required action. Since the techniques and attack patterns used by BumbleBee aligned with the vulnerabilities, I recommended prioritizing these for remediation to reduce the likelihood of exploitation.