Identification and Prioritization of Software Vulnerability and Risk Assessment

Joel Vanta

CyberSecurity Service Provider Internship Program, ICS 296 & 396, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

Problem Statement:

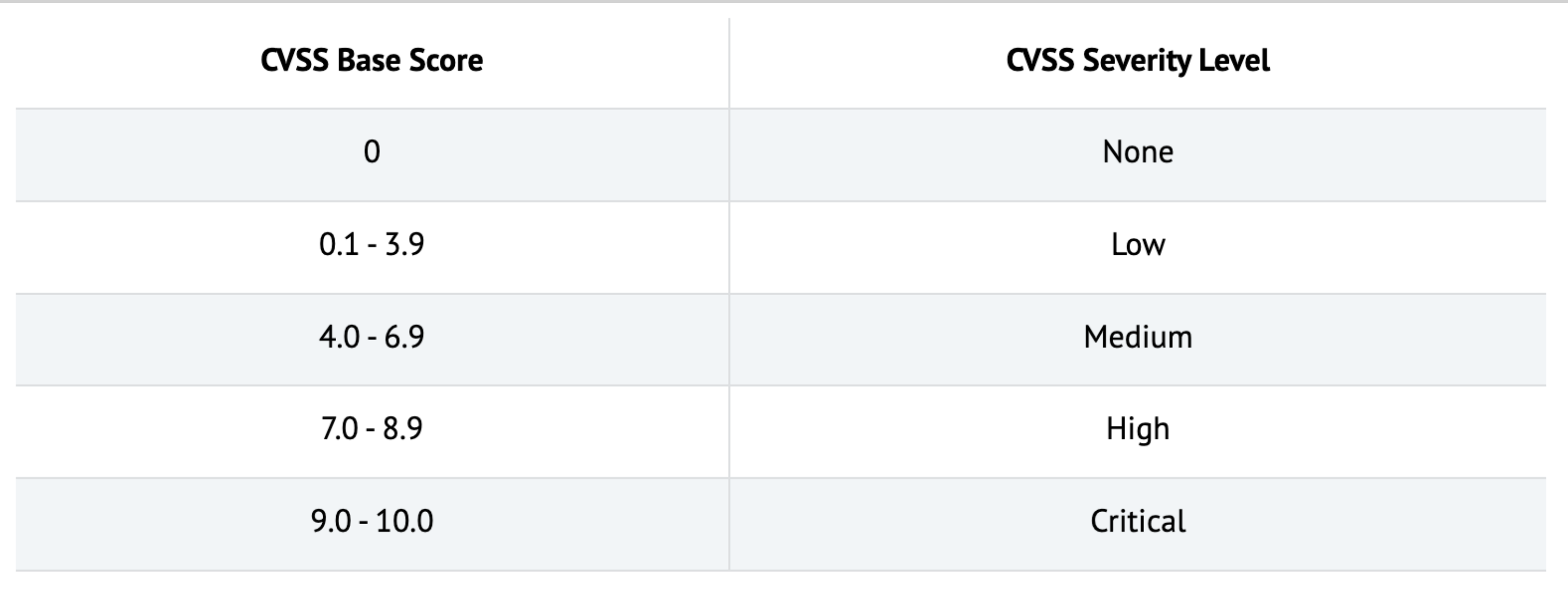
Most people do not know how to identify a cybersecurity threat or how to protect themselves in cases where it will cause harm. Furthermore, there are different vulnerabilities, one should know how to identify and prioritize each of these and make the necessary risk management.

Purpose:

The purpose of identification and prioritizing of software vulnerability is to help and understand the potential effects of these threats and determine how to handle them whenever it is encountered. This study gives a user specific knowledge on how to identify a thereat, and to know its priority and how to handle them so that it can be minimized or avoided in the future.

Approach:

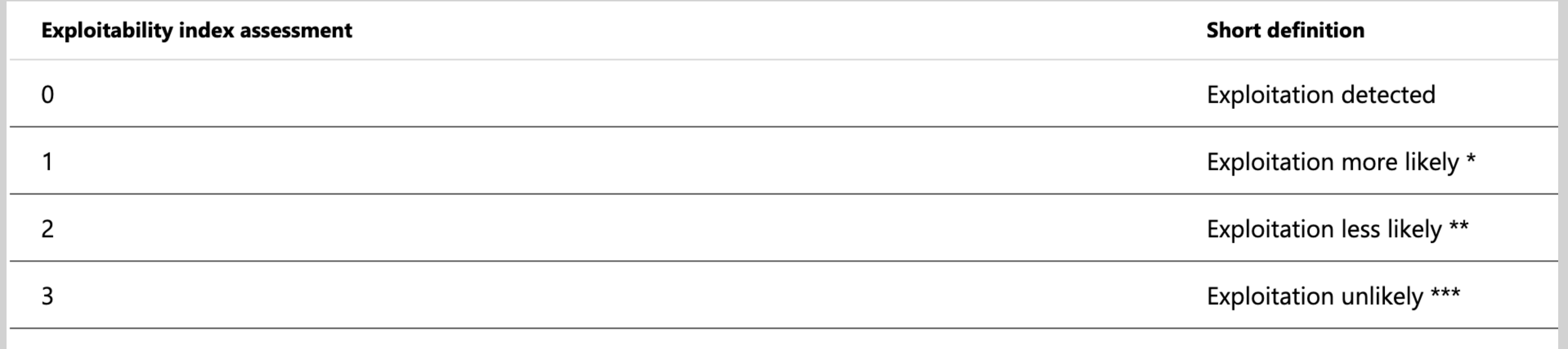
A comparison with two publicly available systems were compared, the Common Vulnerability Scoring System (CVSS) and the Microsoft Exploitability Index. The CVSS has a base score between 0 to 10 and severity level from none to critical. It has the base score metrics of attack vector, attack complexity, privileges required, user interaction, scope, confidentiality, integrity and availability.



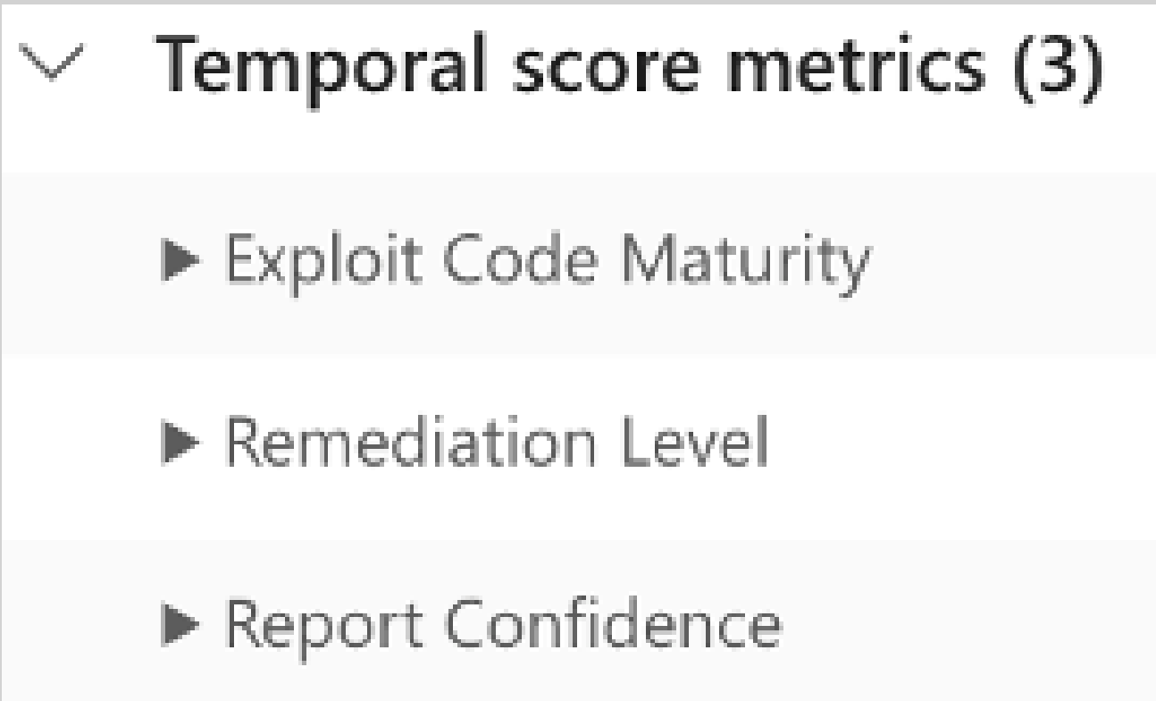
CVSS Base Score	CVSS Severity Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): None
Availability (A): High

The Microsoft Exploitability Index has an index assessment between 0 to 3 and its appropriate definition of exploitation detected to exploitation unlikely. It also includes temporal score metrics such as exploit code maturity, remediation level, and report confidence.



Exploitability index assessment	Short definition
0	Exploitation detected
1	Exploitation more likely *
2	Exploitation less likely **
3	Exploitation unlikely ***



Temporal score metrics (3)

▶ Exploit Code Maturity

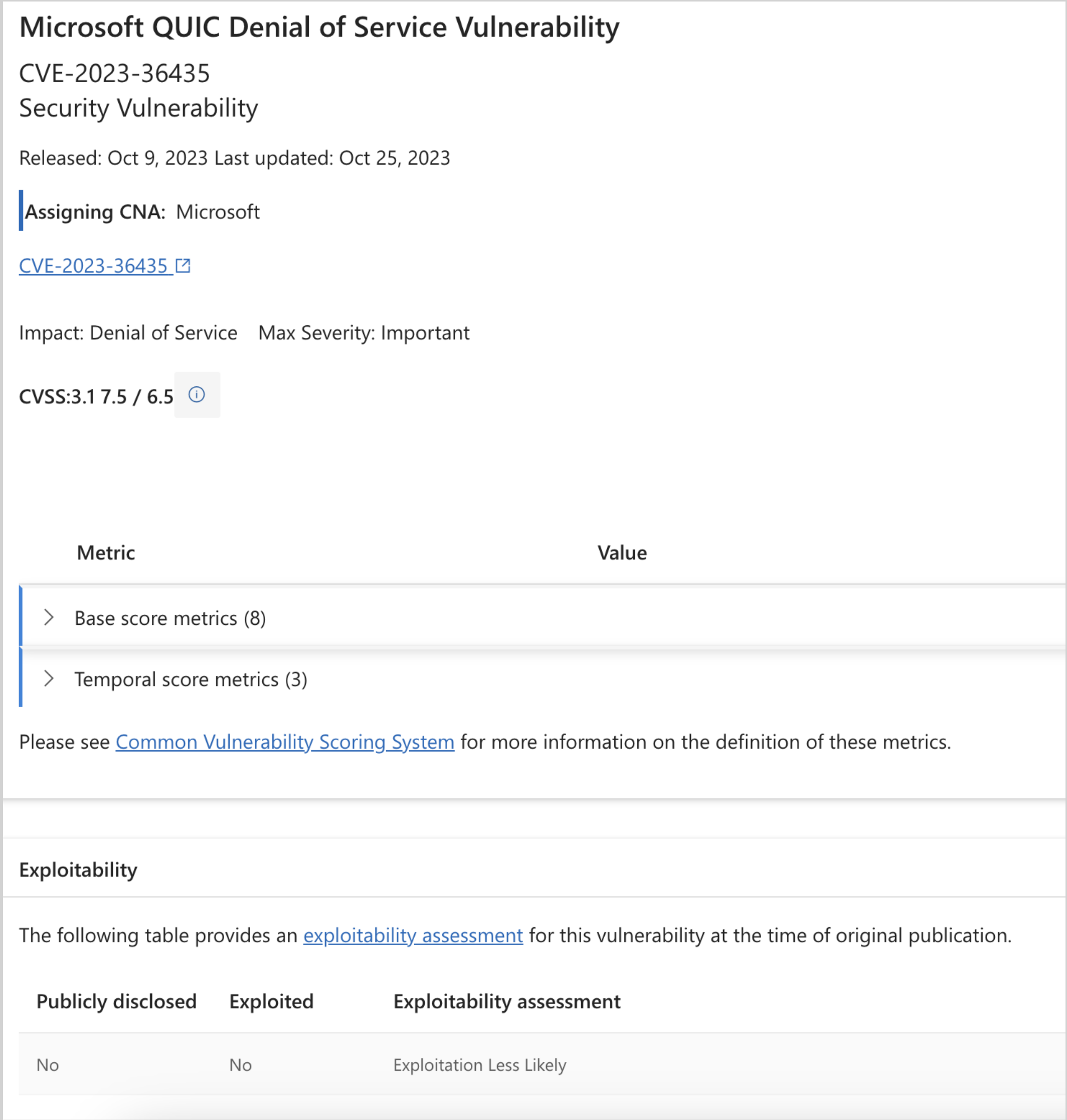
▶ Remediation Level

▶ Report Confidence

INFORMATION & COMPUTER SCIENCES
UNIVERSITY *of* HAWAIʻI *at* MĀNOA

Discussion & Conclusion:

A comparison between the result of the CVSS Base Metrics and the Microsoft Exploitability Index assessment was performed on CVE-2023-36435.



Microsoft QUIC Denial of Service Vulnerability

CVE-2023-36435
Security Vulnerability

Released: Oct 9, 2023 Last updated: Oct 25, 2023

Assigning CNA: Microsoft

CVE-2023-36435

Impact: Denial of Service Max Severity: Important

CVSS:3.1 7.5 / 6.5

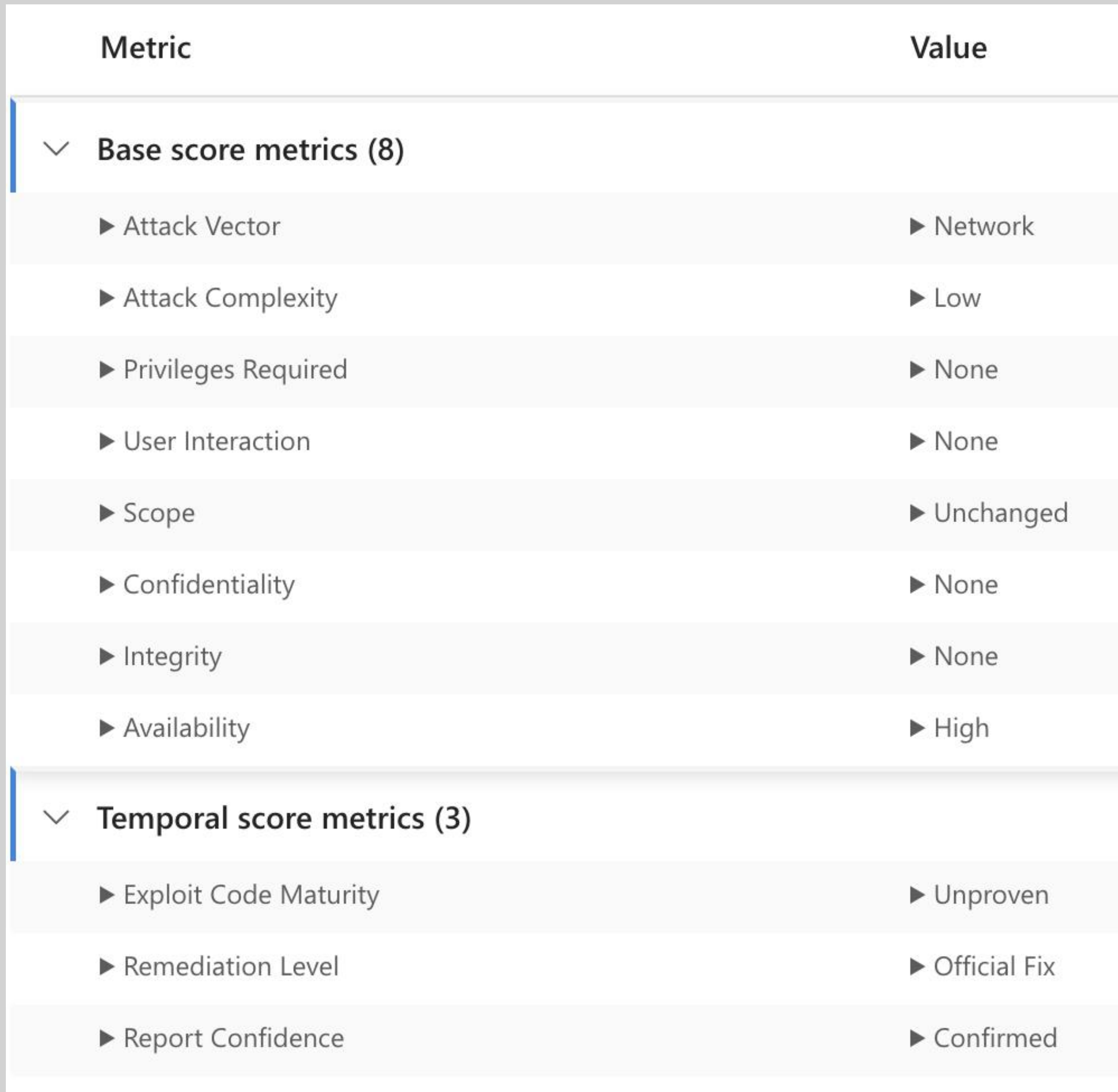
Metric	Value
Base score metrics (8)	
Temporal score metrics (3)	

Please see Common Vulnerability Scoring System for more information on the definition of these metrics.

Exploitability

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly disclosed	Exploited	Exploitability assessment
No	No	Exploitation Less Likely



Metric	Value
Base score metrics (8)	
▶ Attack Vector	▶ Network
▶ Attack Complexity	▶ Low
▶ Privileges Required	▶ None
▶ User Interaction	▶ None
▶ Scope	▶ Unchanged
▶ Confidentiality	▶ None
▶ Integrity	▶ None
▶ Availability	▶ High
Temporal score metrics (3)	
▶ Exploit Code Maturity	▶ Unproven
▶ Remediation Level	▶ Official Fix
▶ Report Confidence	▶ Confirmed

The study found out that there are different ways to prioritize vulnerability. Two of the publicly available tools are the CVSS and the Microsoft Exploitability Index. The Microsoft Security Response Center currently includes the CVSS base score metrics and the Microsoft Exploitability Index. It also includes temporal score metrics which includes the remediation level which is an important factor for prioritization. A typical vulnerability is unpatched when it is initially posted. Several workarounds or hotfixes can be done as a temporary solution until an official patch or upgrade is made.

Path Forward:

The findings of this study can be applied by beginners who want to know how vulnerability are being prioritized. Using CVSS and the Microsoft Exploitability Index, one can make the necessary risk assessment and mitigation whenever any type of vulnerability is encountered. There are prioritization matrices that are available through different vendors. Since most of them are not publicly available, further research and analysis should be done to determine the methods that were used to prioritize vulnerability.

References:

Younis, A. A., & Malaiya, Y. K. (2015). Comparing and evaluating CVSS base metrics and Microsoft Rating System. 2015 IEEE International Conference on Software Quality, Reliability and Security. https://doi.org/10.1109/qrs.2015.44

Microsoft QUIC Denial of Service Vulnerability. Security Update Guide - Microsoft Security Response Center. (2023). https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36435

UNCLASSIFIED/APPROVED FOR PUBLIC RELEASE