淺談CVSS 4.0與弱點分數評估的演變

An Overview of CVSS 4.0 and the Evolution of
Vulnerability Scoring Assessment

Threat Signature Research | Daniel Chiu | Canaan Kao

Speaker

Canaan Kao 任職於 TXOne Networks 擔任 Threat Research Director。他自 2001 年起擔任 DPI / IDS / IPS 工程師。他領導了 MoECC 委託給 NTHU 的 Anti-Botnet 計畫 (2009 - 2013) 並舉辦了 “ Botnet of Taiwan ” (BoT) 研討會 (2009 - 2014)。他在 HITCON 2014 CMT、HITCON 2015 CMT 和 HITCON 2019 發表過演講。他的主要研究興趣是網絡安全、入侵偵測系統、逆向工程、惡意軟體偵測和嵌入式系統。

Daniel Chiu 任職於 TXOne Networks，擔任Threat Signature Research Team Manager，自2013就業以來專注在DPI的改進和DPI特徵碼的撰寫，目前帶領團隊分析網路漏洞、開發IPS rule和ICS Protocol相關研究。 興趣:研究網路攻擊手法和改進防禦方法。

CONTENTS

01 | Introduction

- Brief overview of CVSS (Common Vulnerability Scoring System)
- Historical context

02 | The changes for CVSS 4.0

- Limitations of earlier version
- Key Features of CVSS 4.0

03 | Scoring Metrics Breakdown

- Base Metrics
- Temporal Metrics / Threat Metrics
- Environmental Metrics
- Supplemental Metrics

04 | Case Study

Utilize a case study for simulation, analyze vulnerability, extract features required for CVSS, and calculate the score.

05 | Conclusion

06 | Q&A

Introduction

Common Vulnerability Scoring System, CVSS

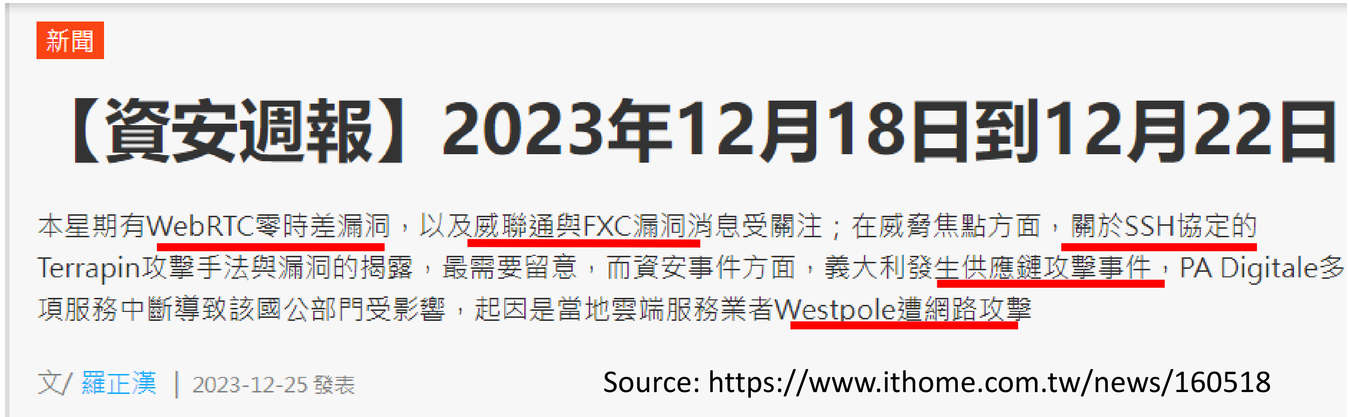
A vendor agnostic, industry open standard
解決不同資安供應商間不相容、封閉及缺乏統一標準的弱點評分方式，避免單一個弱點有多種的解讀方式和不同的評分

To convey vulnerability severity
使用共同的語言傳遞弱點的嚴重性和影響

Help determine urgency and priority of response.
提供弱點整體性的嚴重性和風險評分，幫助使用者排序弱點處理優先順序

Usable and understandable by anyone
資安專業人員、管理者以及一般使用者，都能夠理解，並用相同的語言討論一個弱點

Vulnerability Information



新聞

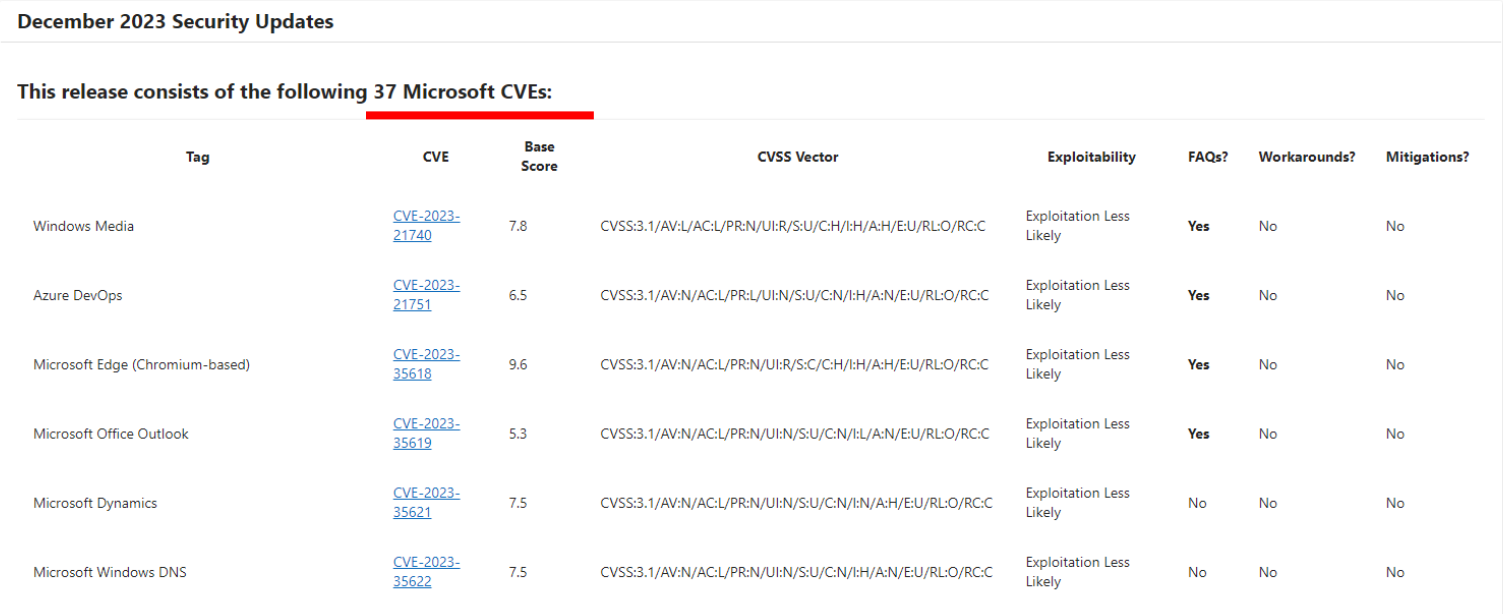
【資安週報】2023年12月18日到12月22日

本星期有WebRTC零時差漏洞，以及威聯通與FXC漏洞消息受關注；在威脅焦點方面，關於SSH協定的Terrapin攻擊手法與漏洞的揭露，最需要留意，而資安事件方面，義大利發生供應鏈攻擊事件，PA Digitale多項服務中斷導致該國公部門受影響，起因是當地雲端服務業者Westpole遭網路攻擊

文/ 羅正漢 | 2023-12-25 發表

Source: https://www.ithome.com.tw/news/160518

28,803 new CVEs added in 2023, more then 550 CVEs be published weekly in average



December 2023 Security Updates

This release consists of the following 37 Microsoft CVEs:

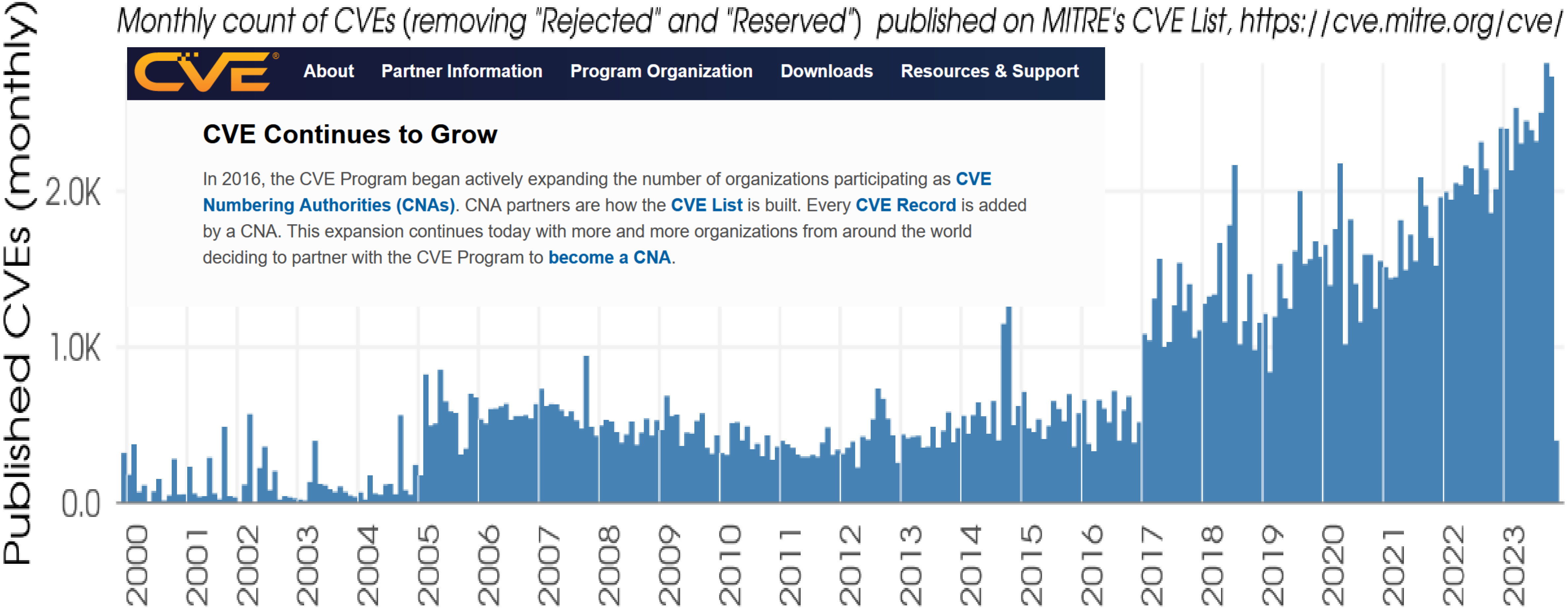
Tag	CVE	Base Score	CVSS Vector	Exploitability	FAQs?	Workarounds?	Mitigations?
Windows Media	CVE-2023-21740	7.8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	Exploitation Less Likely	**Yes**	No	No
Azure DevOps	CVE-2023-21751	6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C	Exploitation Less Likely	**Yes**	No	No
Microsoft Edge (Chromium-based)	CVE-2023-35618	9.6	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C	Exploitation Less Likely	**Yes**	No	No
Microsoft Office Outlook	CVE-2023-35619	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C	Exploitation Less Likely	**Yes**	No	No
Microsoft Dynamics	CVE-2023-35621	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C	Exploitation Less Likely	No	No	No
Microsoft Windows DNS	CVE-2023-35622	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C	Exploitation Less Likely	No	No	No

Source: https://msrc.microsoft.com/update-guide/releaseNote/2023-dec

- It is very important to quickly assess the damage a vulnerability can inflict on an organization
- CVSS captures the technical characteristics of vulnerabilities, and outputs numerical scores indicating the severity of a vulnerability

Monthly counts of CVE publications (MITRE CVE List)

Monthly count of CVEs (removing "Rejected" and "Reserved") published on MITRE's CVE List, https://cve.mitre.org/cve/



CVE Continues to Grow

In 2016, the CVE Program began actively expanding the number of organizations participating as **CVE Numbering Authorities (CNAs)**. CNA partners are how the **CVE List** is built. Every **CVE Record** is added by a CNA. This expansion continues today with more and more organizations from around the world deciding to partner with the CVE Program to **become a CNA**.

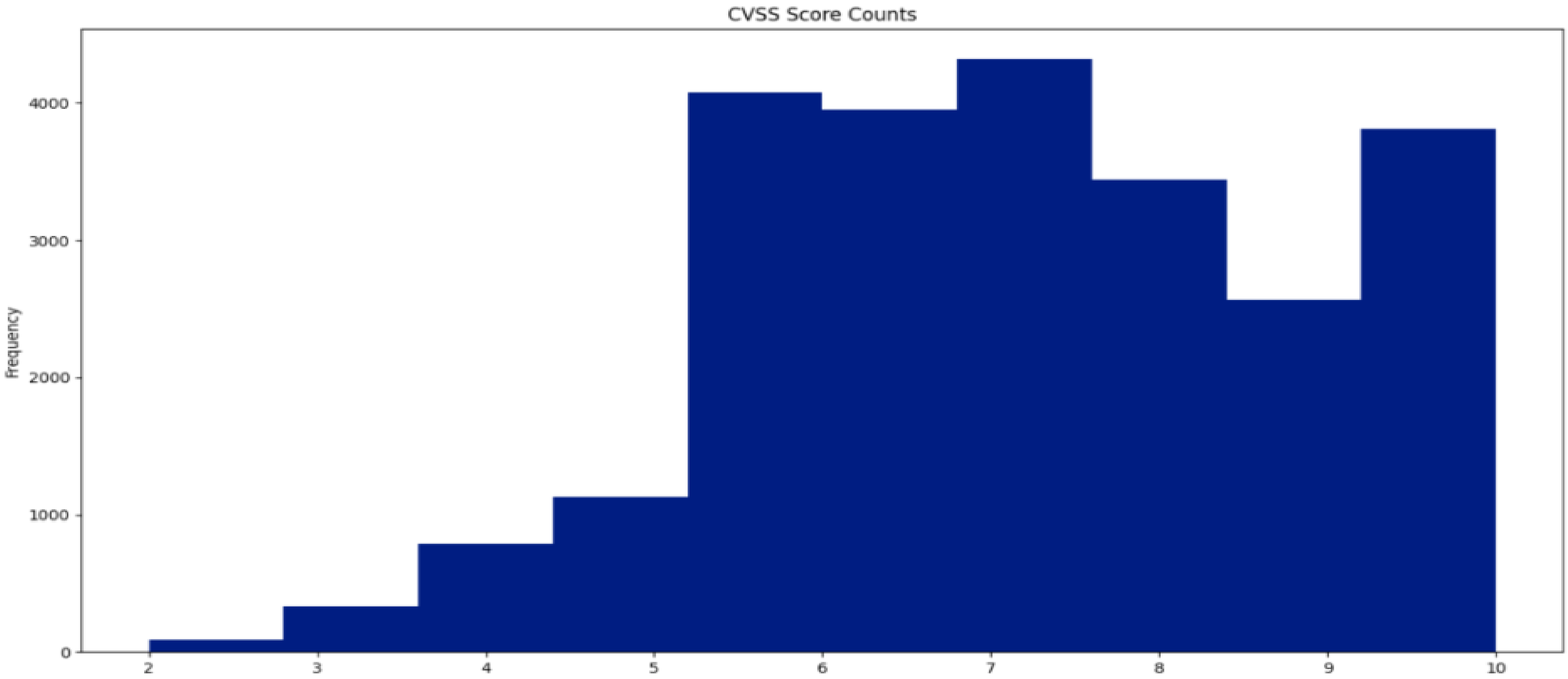
Source: https://first.org/epss/data_stats, 2023-11-06

NVD Vulnerability Severity Ratings (https://nvd.nist.gov/vuln-metrics/cvss)

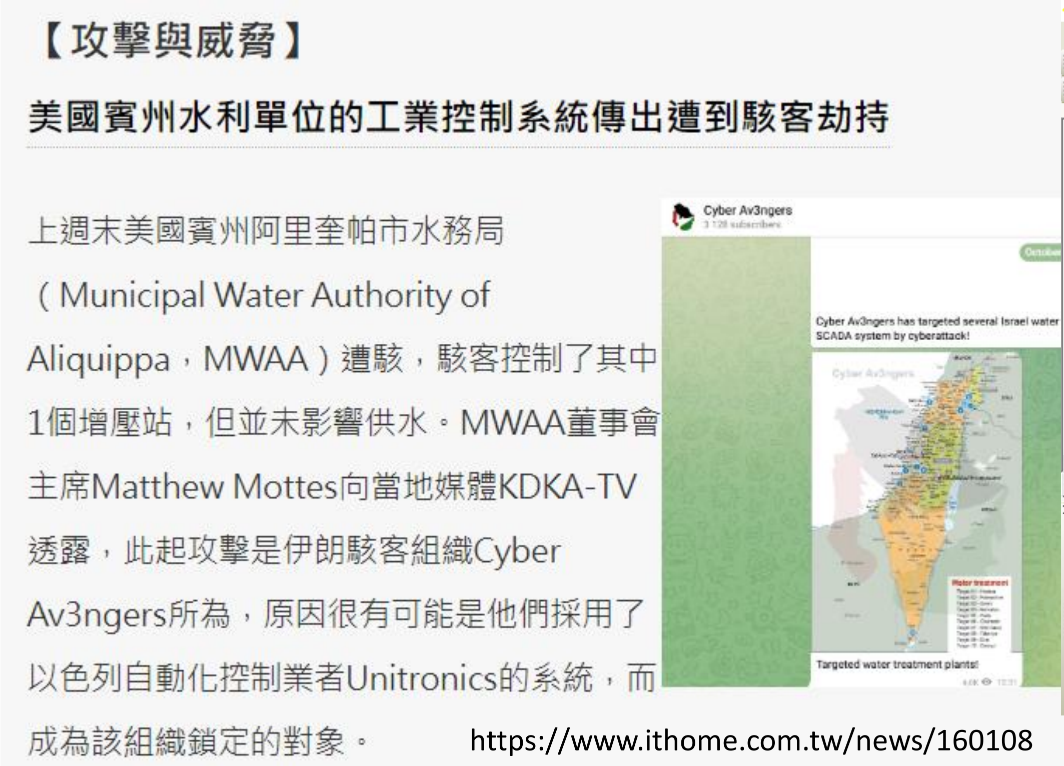
CVSS v2.0 Ratings		CVSS v3.x Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

The average CVSS score in 2022 was 7.19 **(High !!)**.

source: https://jerrygamblin.com/2023/01/01/2022-cve-data-review/



Using a score quickly indicates the severity of a vulnerability



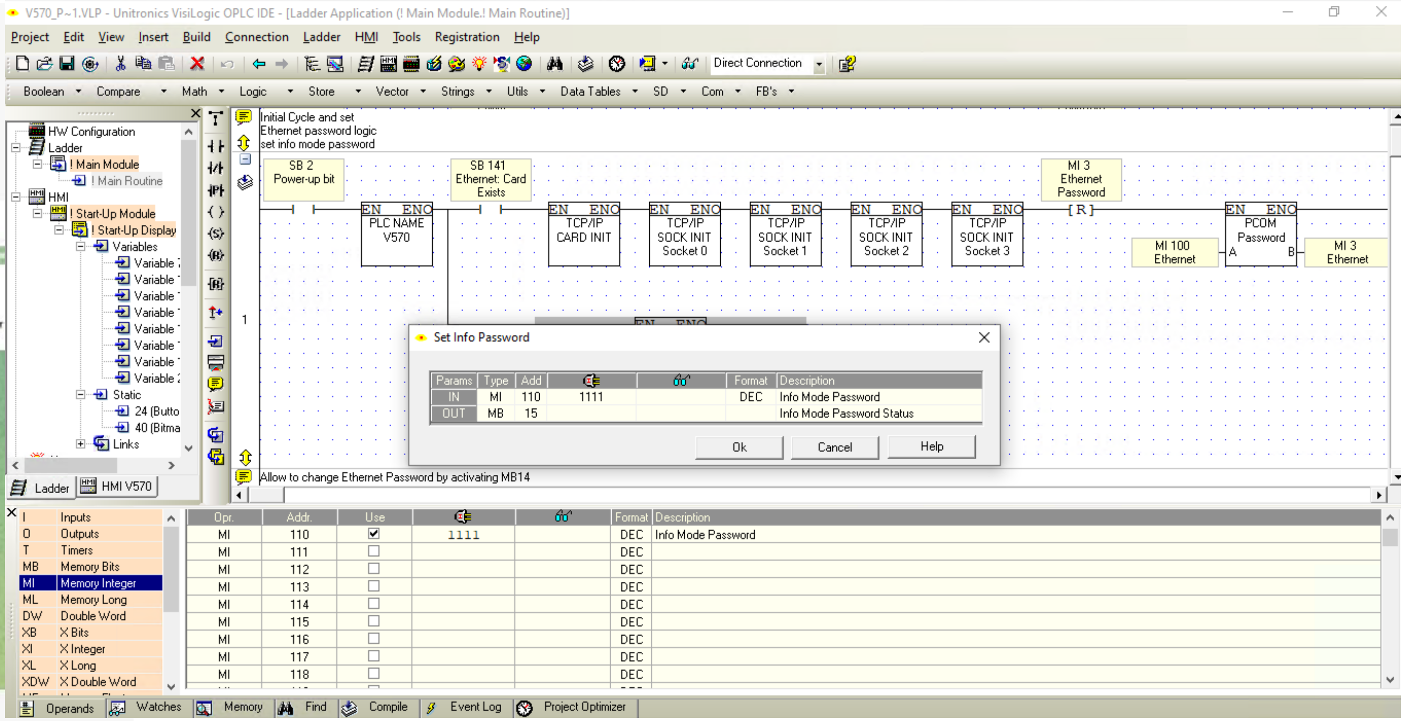
【攻擊與威脅】

美國賓州水利單位的工業控制系統傳出遭到駭客劫持

上週末美國賓州阿里奎帕市水務局（Municipal Water Authority of Aliquippa，MWAA）遭駭，駭客控制了其中1個增壓站，但並未影響供水。MWAA董事會主席Matthew Mottes向當地媒體KDKA-TV透露，此起攻擊是伊朗駭客組織Cyber Av3ngers所為，原因很有可能是他們採用了以色列自動化控制業者Unitronics的系統，而成為該組織鎖定的對象。

Cyber Av3ngers
Cyber Av3ngers has targeted several Israel water SCADA system by cyberattack!
Targeted water treatment plants!

https://www.ithome.com.tw/news/160108



V570_P~1.VLP - Unitronics VisiLogic OPLC IDE - [Ladder Application (! Main Module.! Main Routine)]

Initial Cycle and set
Ethernet password logic
set info mode password

Set Info Password

Params	Type	Add			Format	Description
IN	MI	110	1111		DEC	Info Mode Password
OUT	MB	15				Info Mode Password Status

Ok Cancel Help

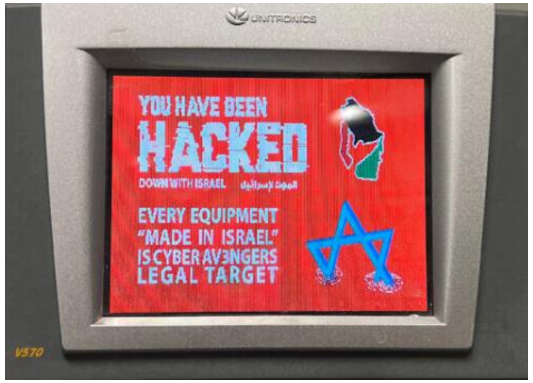
Allow to change Ethernet Password by activating MB14

Opr.	Addr.	Use			Format	Description
MI	110	☑	1111		DEC	Info Mode Password
MI	111	□			DEC	
MI	112	□			DEC	
MI	113	□			DEC	
MI	114	□			DEC	
MI	115	□			DEC	
MI	116	□			DEC	
MI	117	□			DEC	
MI	118	□			DEC	

CVE-2023-6448 Detail

Unitronics VisiLogic before version 9.9.00, used in Vision and Samba PLCs and HMIs, uses a default administrative password. An unauthenticated attacker with network access can take administrative control of a vulnerable system.

Base Score: 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

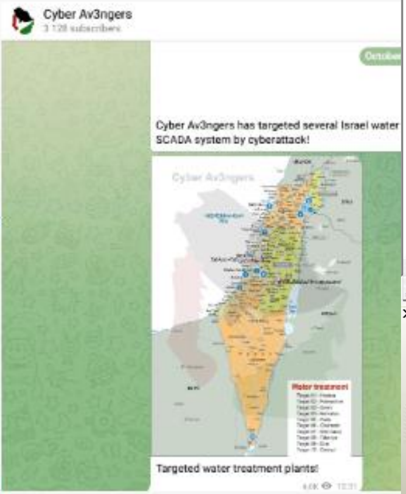


Using a score quickly indicates the severity of a vulnerability

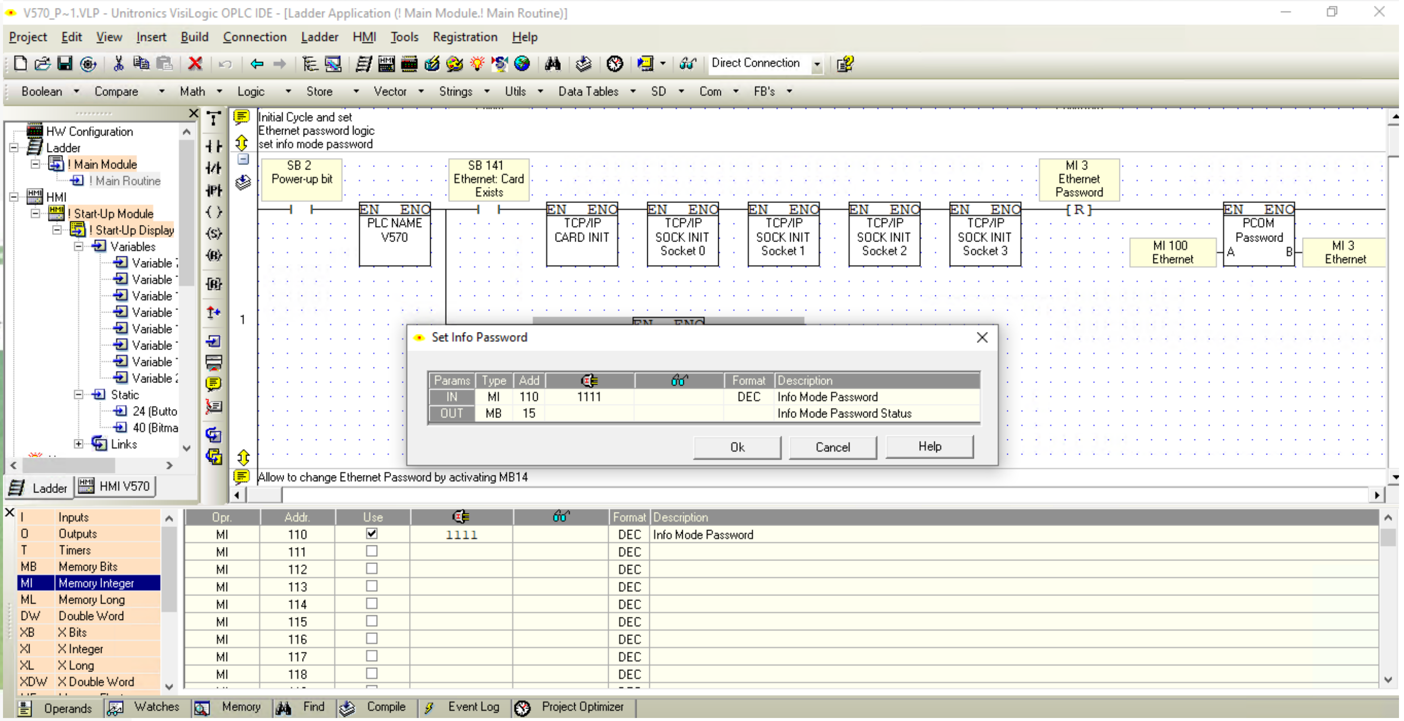
【攻擊與威脅】

美國賓州水利單位的工業控制系統傳出遭到駭客劫持

上週末美國賓州阿里奎帕市水務局（Municipal Water Authority of Aliquippa，MWAA）遭駭，駭客控制了其中1個增壓站，但並未影響供水。MWAA董事會主席Matthew Mottes向當地媒體KDKA-TV透露，此起攻擊是伊朗駭客組織Cyber Av3ngers所為，原因很有可能是他們採用了以色列自動化控制業者Unitronics的系統，而成為該組織鎖定的對象。


Cyber Av3ngers
Cyber Av3ngers has targeted several Israel water SCADA system by cyberattack!
Targeted water treatment plants!

https://www.ithome.com.tw/news/160108


V570_P~1.VLP - Unitronics VisiLogic OPLC IDE - [Ladder Application (! Main Module.! Main Routine)]
Project Edit View Insert Build Connection Ladder HMI Tools Registration Help
Direct Connection
Boolean Compare Math Logic Store Vector Strings Utils Data Tables SD Com FB's
HW Configuration
Ladder
! Main Module
! Main Routine
HMI
! Start-Up Module
! Start-Up Display
Variables
Static
Links
Ladder
HMI V570
SB 2 Power-up bit
PLC NAME V570
SB 141 Ethernet: Card Exists
TCP/IP CARD INIT
TCP/IP SOCK INIT Socket 0
TCP/IP SOCK INIT Socket 1
TCP/IP SOCK INIT Socket 2
TCP/IP SOCK INIT Socket 3
MI 3 Ethernet Password
MI 100 Ethernet
PCOM Password
MI 3 Ethernet
Inputs
Outputs
Timers
Memory Bits
Memory Integer
Memory Long
Double Word
X Bits
X Integer
X Long
X Double Word
Operands Watches Memory Find Compile Event Log Project Optimizer

Initial Cycle and set
Ethernet password logic
set info mode password

Set Info Password

Params	Type	Add			Format	Description
IN	MI	110	1111		DEC	Info Mode Password
OUT	MB	15				Info Mode Password Status

Ok Cancel Help

Allow to change Ethernet Password by activating MB14

Opr.	Addr.	Use			Format	Description
MI	110	☑	1111		DEC	Info Mode Password
MI	111	□			DEC	
MI	112	□			DEC	
MI	113	□			DEC	
MI	114	□			DEC	
MI	115	□			DEC	
MI	116	□			DEC	
MI	117	□			DEC	
MI	118	□			DEC	

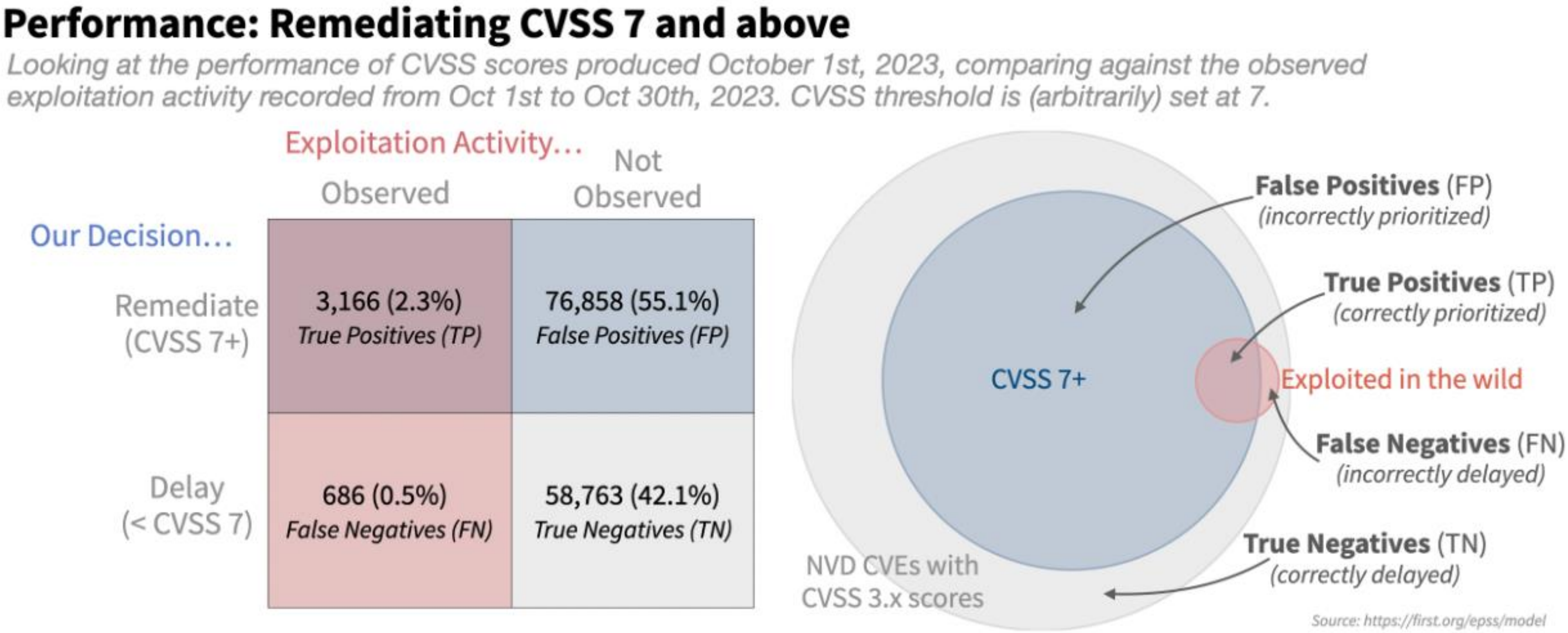
CVE-2023-6448 Detail

Unitronics VisiLogic before version 9.9.00, used in Vision and Samba PLCs and HMIs, uses a default administrative password. An unauthenticated attacker with network access can take administrative control of a vulnerable system.

Base Score: 9.8 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Estimate severity quickly through scores

Only a small subset (2%-5%) of published vulnerabilities is ever seen to be exploited in the wild



Performance: Remediating CVSS 7 and above

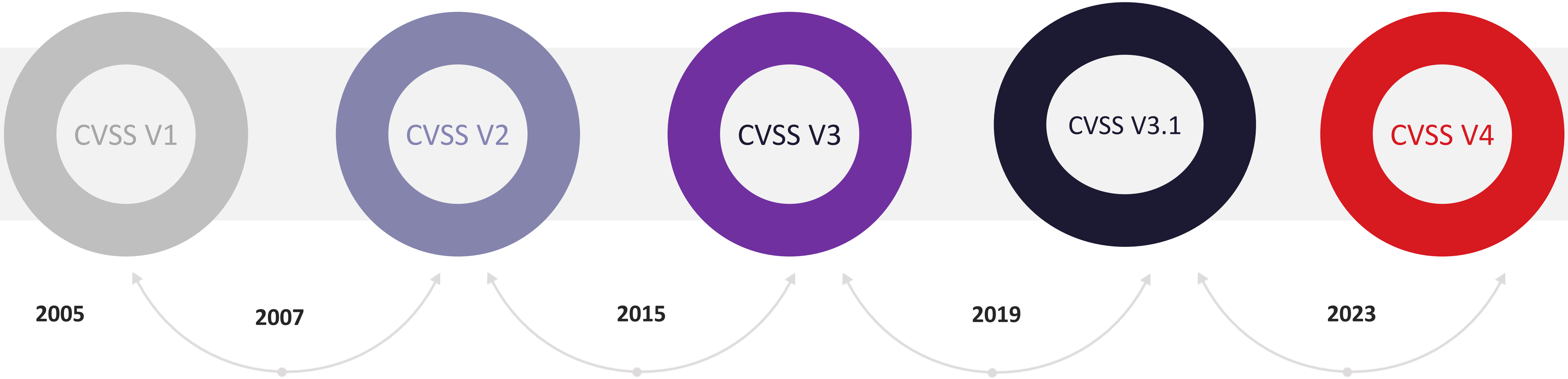
Looking at the performance of CVSS scores produced October 1st, 2023, comparing against the observed exploitation activity recorded from Oct 1st to Oct 30th, 2023. CVSS threshold is (arbitrarily) set at 7.

Our Decision…	Exploitation Activity…	
	Observed	Not Observed
Remediate (CVSS 7+)	3,166 (2.3%) *True Positives (TP)*	76,858 (55.1%) *False Positives (FP)*
Delay (< CVSS 7)	686 (0.5%) *False Negatives (FN)*	58,763 (42.1%) *True Negatives (TN)*

Source: https://first.org/epss/model

https://www.first.org/

Historical Context



Reduce inconsistencies, provide additional granularity, and reflect more accurately

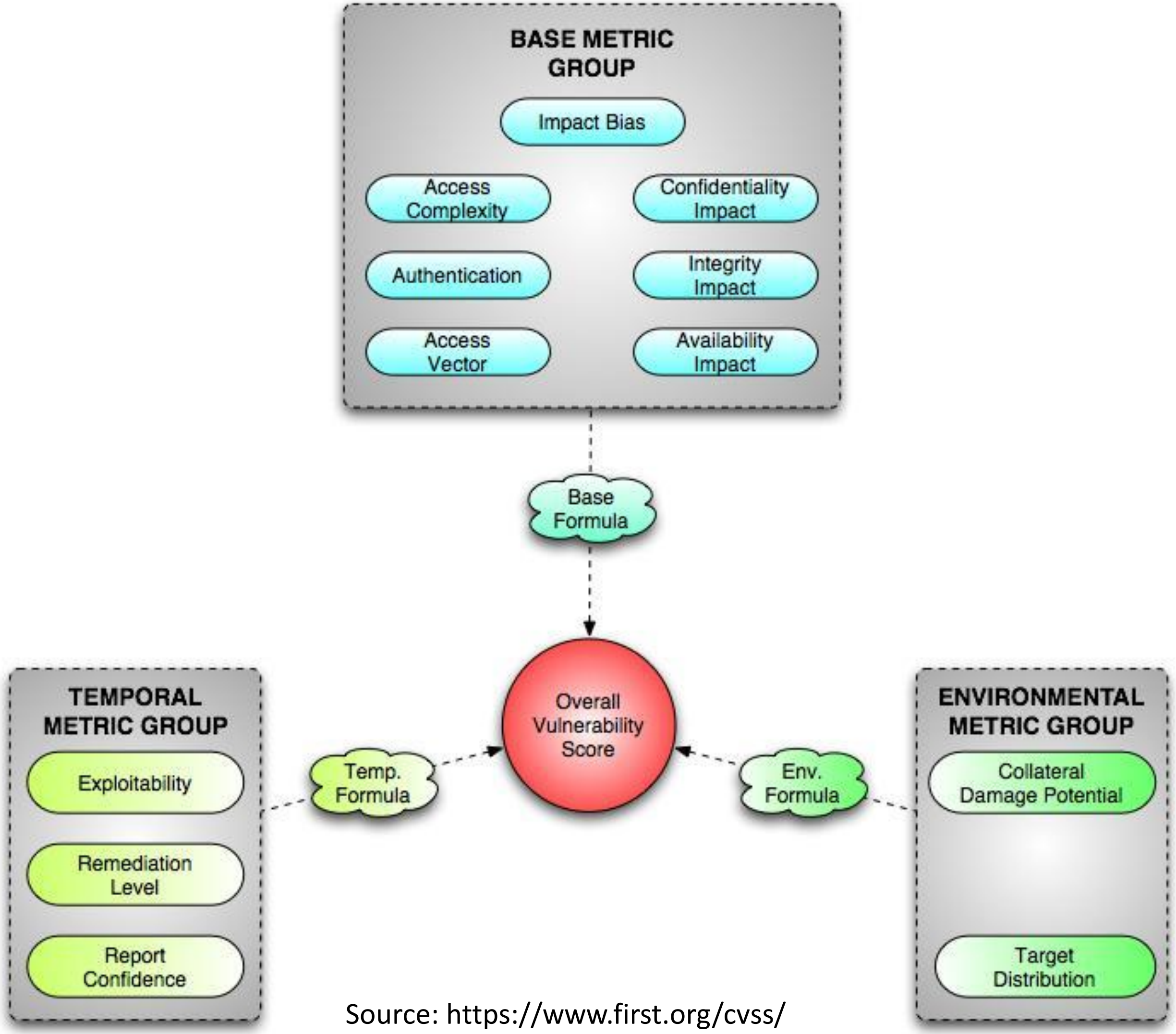
Added the concept of "scope" to handle scoring of vulnerabilities that exist within a software component but affect separate components

- Clarified and improved upon version 3.0 without introducing new metrics.
- *CVSS is designed to measure the severity of a vulnerability and should not be used alone to assess risk.*

- Emphasizes the importance of using threat intelligence and environmental indicators for accurate scoring.
- Added OT Safety Metrics.

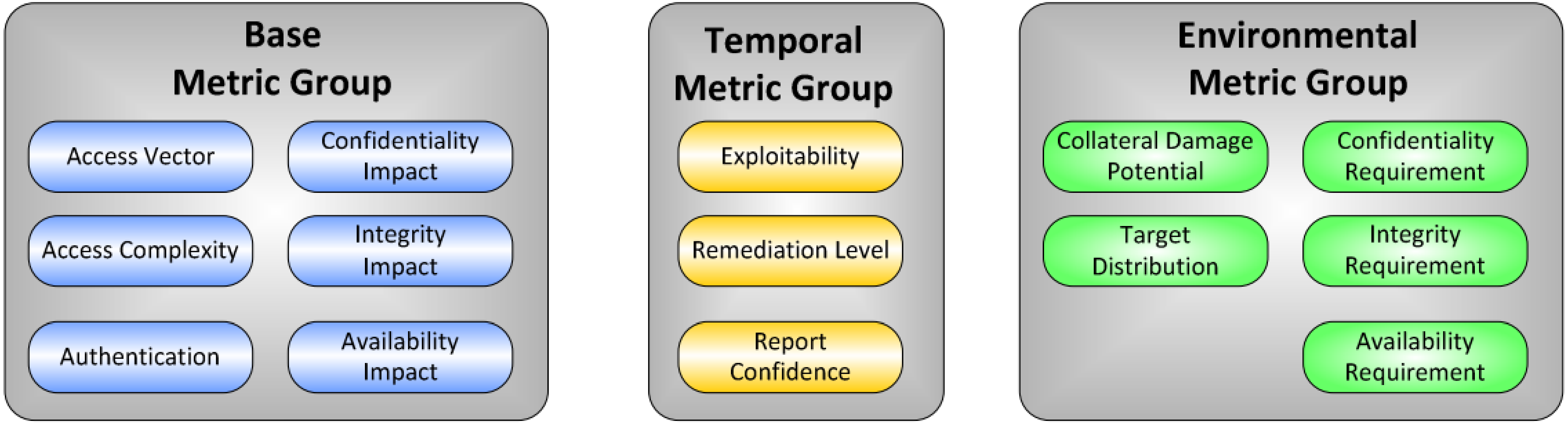
The changes for CVSS 4.0

The Metrics Group of CVSS v1 (2005)



Source: https://www.first.org/cvss/

The Metrics Group of CVSS v2 (2007)



Base Metric Group

- Access Vector
- Confidentiality Impact
- Access Complexity
- Integrity Impact
- Authentication
- Availability Impact

Temporal Metric Group

- Exploitability
- Remediation Level
- Report Confidence

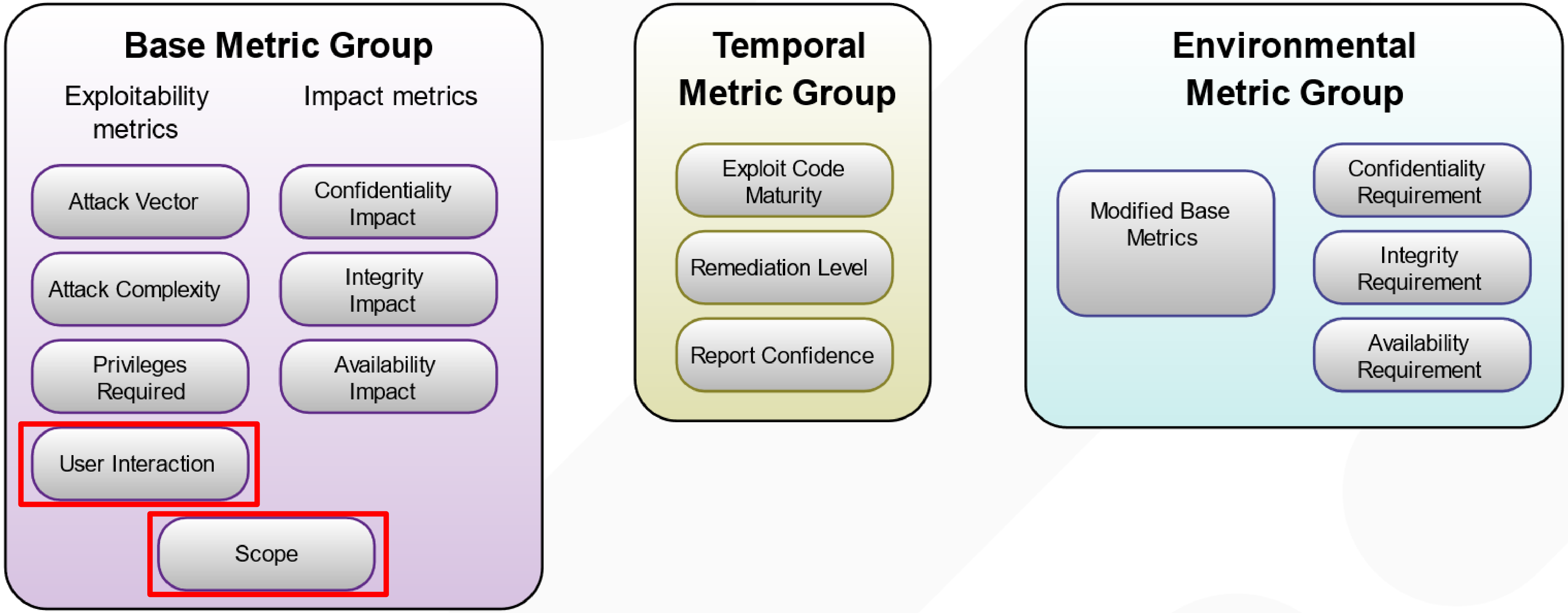
Environmental Metric Group

- Collateral Damage Potential
- Confidentiality Requirement
- Target Distribution
- Integrity Requirement
- Availability Requirement

AV:N/AC:L/Au:N/C:N/I:N/A:C

Source: https://www.first.org/cvss/

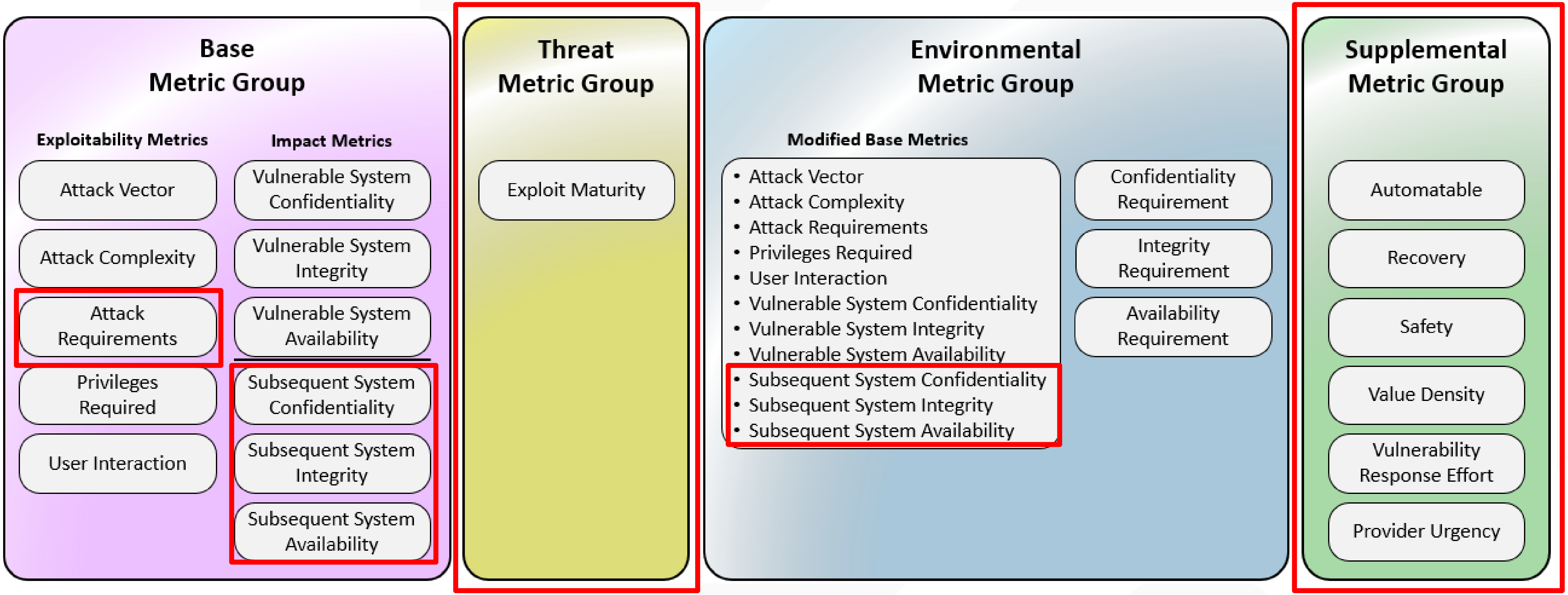
The Metrics Group of CVSS v3 (2015)



Source: https://www.first.org/cvss/

The Metrics Group of CVSS v4 (2023)

New



Base Metric Group

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction

Impact Metrics

- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

Threat Metric Group

- Exploit Maturity

Environmental Metric Group

Modified Base Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Supplemental Metric Group

- Automatable
- Recovery
- Safety
- Value Density
- Vulnerability Response Effort
- Provider Urgency

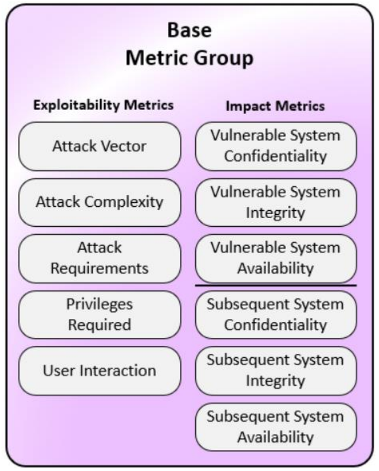
Source: https://www.first.org/cvss/

CVSS v4 is not just the Base Score

New

CVSS-B

Base Score



Base
Metric Group

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction

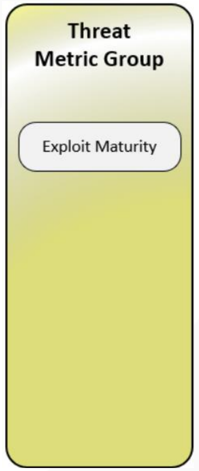
Impact Metrics

- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

+

CVSS-BT

Base + Threat Score



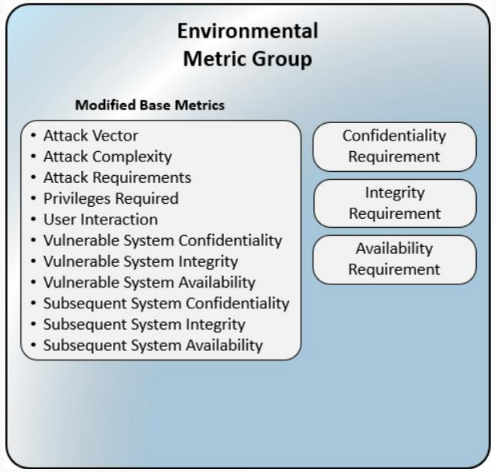
Threat
Metric Group

- Exploit Maturity

+

CVSS-BTE

Base + Threat + Environmental Score

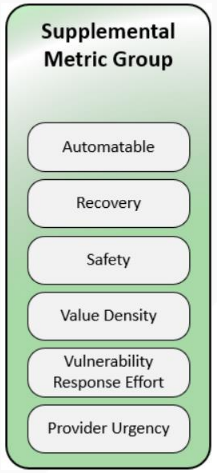


Environmental
Metric Group

Modified Base Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement



Supplemental
Metric Group

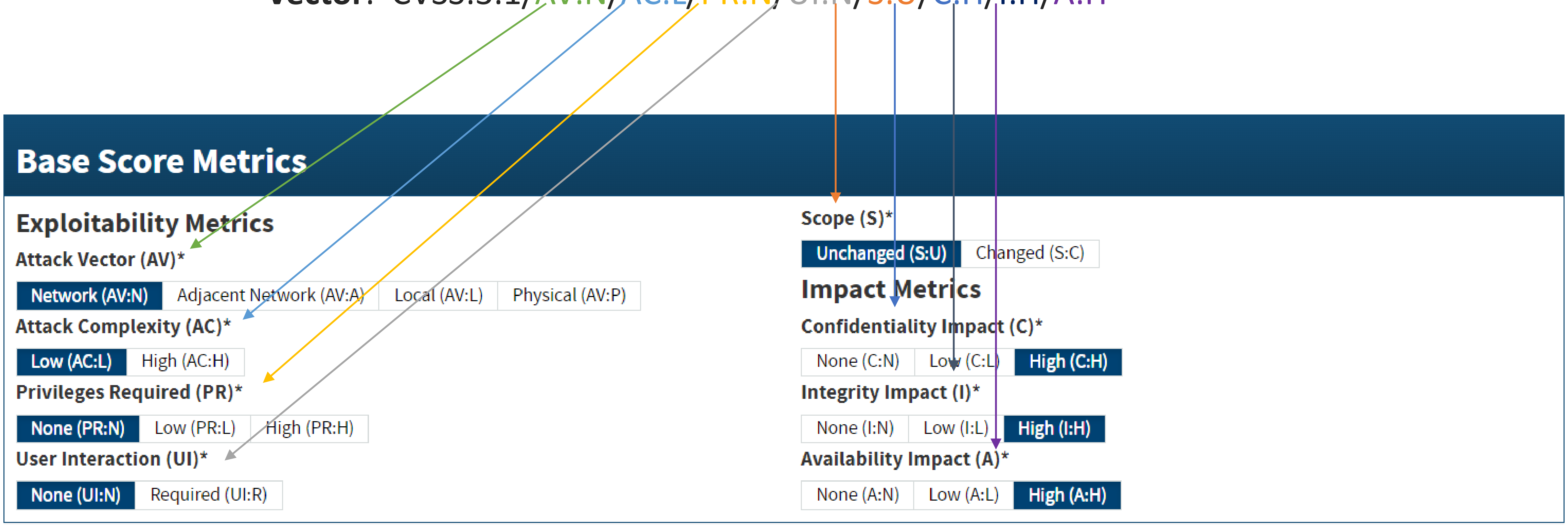
- Automatable
- Recovery
- Safety
- Value Density
- Vulnerability Response Effort
- Provider Urgency

No impact on final CVSS score, Used as additional insight into the characteristics of a vulnerability

CVSS Format (v3.1)

Base Score: 9.8 CRITICAL (score ranging from 0.0 to 10.0)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*

[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*

[✓ None (UI:N)] Required (UI:R)

Scope (S)*

[✓ Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) [✓ High (C:H)]

Integrity Impact (I)*

None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*

None (A:N) Low (A:L) [✓ High (A:H)]

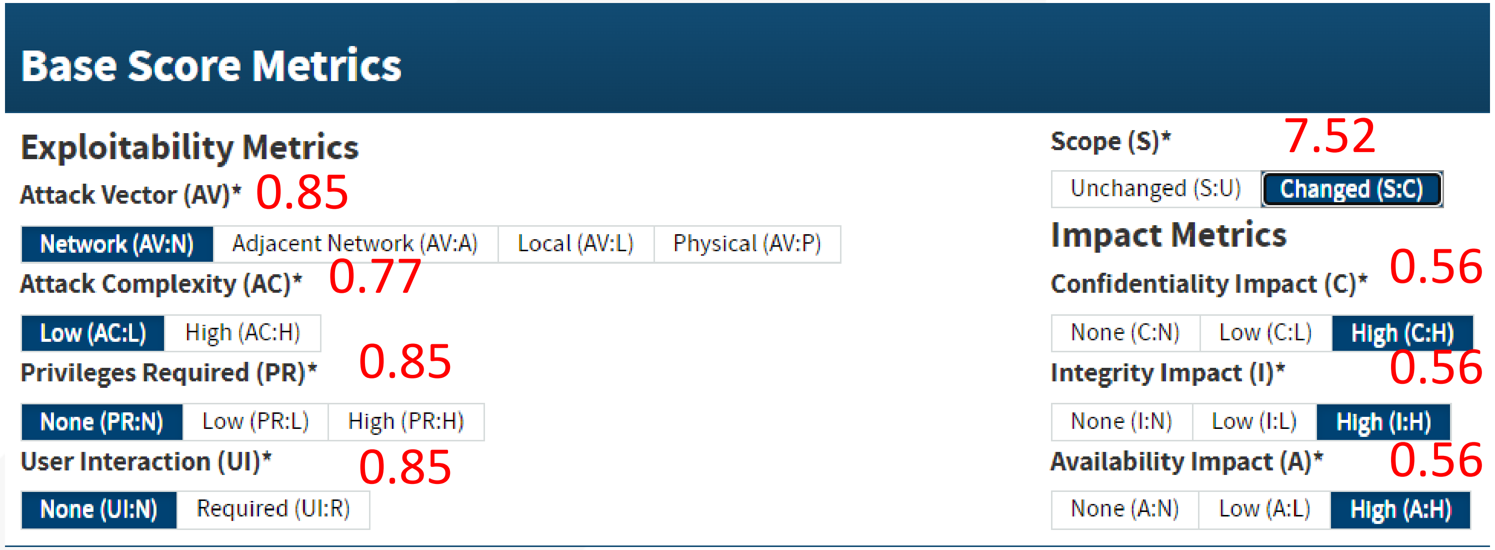
Based on the characteristics of the vulnerability, match each one to its corresponding indicator

CVSS v3 Formula

```
CVSS31.Weight = {
  AV:   { N: 0.85,  A: 0.62,  L: 0.55,  P: 0.2},
  AC:   { H: 0.44,  L: 0.77},
  PR:   { U:      {N: 0.85,  L: 0.62,  H: 0.27},
          C:      {N: 0.85,  L: 0.68,  H: 0.5}},
  UI:   { N: 0.85,  R: 0.62},
  S:    { U: 6.42,  C: 7.52},
  CIA:  { N: 0,     L: 0.22,  H: 0.56},

  E:    { X: 1,     U: 0.91,  P: 0.94,  F: 0.97,  H: 1},
  RL:   { X: 1,     O: 0.95,  T: 0.96,  W: 0.97,  U: 1},
  RC:   { X: 1,     U: 0.92,  R: 0.96,  C: 1},

  CIAR: { X: 1,     L: 0.5,   M: 1,     H: 1.5}
};
```



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)* 0.85

[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)* 0.77

[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)* 0.85

[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)* 0.85

[✓ None (UI:N)] Required (UI:R)

Scope (S)* 7.52

Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

Confidentiality Impact (C)* 0.56

None (C:N) Low (C:L) [✓ High (C:H)]

Integrity Impact (I)* 0.56

None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)* 0.56

None (A:N) Low (A:L) [✓ High (A:H)]

Impact Sub Score = $1 - [(1 - \mathit{ImpactConf}) \times (1 - \mathit{ImpactInteg}) \times (1 - \mathit{ImpactAvail})]$ = 0.914816

if (S === 'U‘) { impact = metricWeightS * iss;} = 5.87311872

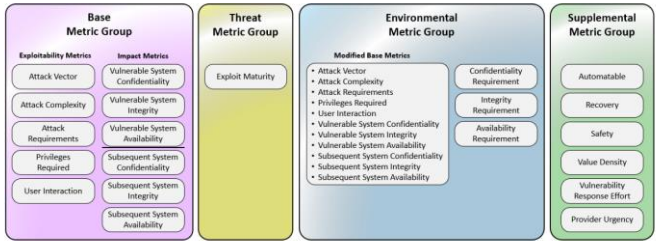
else { impact = metricWeightS * (iss - 0.029) - 3.25 * Math.pow(iss - 0.02, 15);} = 6.0477304915445185

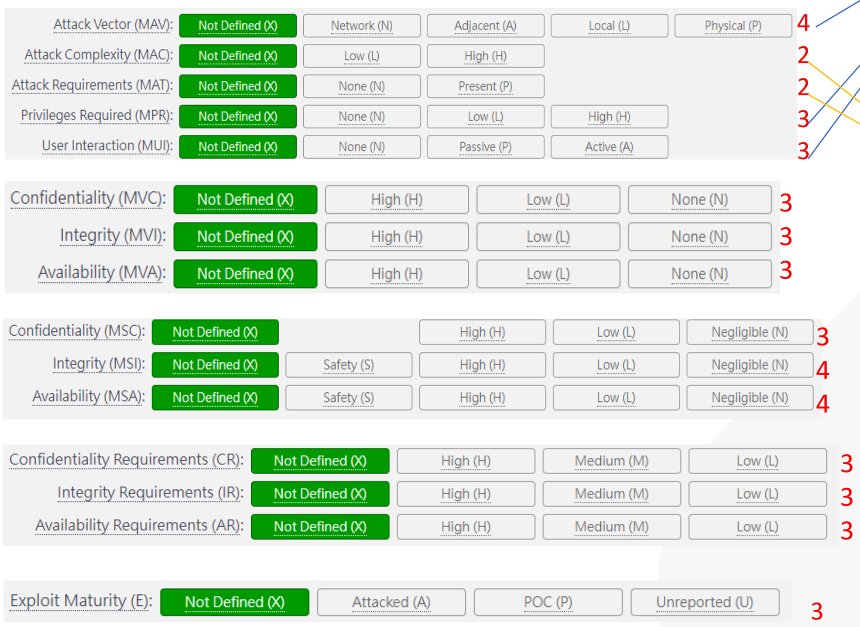
Exploitability = 8.22 $\times \mathit{AttackVector} \times \mathit{AttackComplexity} \times \mathit{PrivilegeRequired} \times \mathit{UserInteraction}$ = 3.887042775

```
if (S === 'U') {
    baseScore = CVSS31.roundUp1(Math.min((exploitability + impact), 10)); = 9.8
  } else {
    baseScore = CVSS31.roundUp1(Math.min(CVSS31.scopeCoefficient * (exploitability + impact), 10)); = 10
```

CVSS v4.0 Formula

New





Attack Vector (MAV):	Not Defined (X)	Network (N)	Adjacent (A)	Local (L)	Physical (P)	4
Attack Complexity (MAC):	Not Defined (X)	Low (L)	High (H)			2
Attack Requirements (MAT):	Not Defined (X)	None (N)	Present (P)			2
Privileges Required (MPR):	Not Defined (X)	None (N)	Low (L)	High (H)		3
User Interaction (MUI):	Not Defined (X)	None (N)	Passive (P)	Active (A)		3
Confidentiality (MVC):	Not Defined (X)	High (H)	Low (L)	None (N)		3
Integrity (MVI):	Not Defined (X)	High (H)	Low (L)	None (N)		3
Availability (MVA):	Not Defined (X)	High (H)	Low (L)	None (N)		3
Confidentiality (MSC):	Not Defined (X)		High (H)	Low (L)	Negligible (N)	3
Integrity (MSI):	Not Defined (X)	Safety (S)	High (H)	Low (L)	Negligible (N)	4
Availability (MSA):	Not Defined (X)	Safety (S)	High (H)	Low (L)	Negligible (N)	4
Confidentiality Requirements (CR):	Not Defined (X)	High (H)	Medium (M)	Low (L)		3
Integrity Requirements (IR):	Not Defined (X)	High (H)	Medium (M)	Low (L)		3
Availability Requirements (AR):	Not Defined (X)	High (H)	Medium (M)	Low (L)		3
Exploit Maturity (E):	Not Defined (X)	Attacked (A)	POC (P)	Unreported (U)		3

36 vectors => 3 Levels

EQ1 → AV/PR/UI with 3 levels (Exploitability)

Levels	Highest Severity Vector(s)
0	AV:N/PR:N/UI:N
1	AV:A/PR:N/UI:N or AV:N/PR:L/UI:N or AV:N/PR:N:/UI:P
2	AV:P/PR:N/UI:N or AV:A/PR:L/UI:P

EQ2 → AC/AT with 2 (Complexity)

Levels	Highest Severity Vector(s)
0	AC:L/AT:N
1	AC:L/AT:P or AC:H/AT:N

EQ3 → VC/VI/VA with 3 levels (Impact)

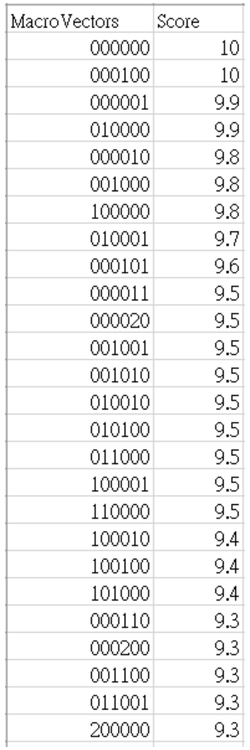
EQ4 → SC/SI/SA with 3 levels (Subsequent system Impact)

EQ5 → E with 3 levels (Exploitation)

EQ6 → VC/VI/VA+CR/CI/CA with 2 levels (Security requirements)

Comparing vectors represented by experts

EQ1,2,3,4,5,6
0,0,0,0,0,0 => 10

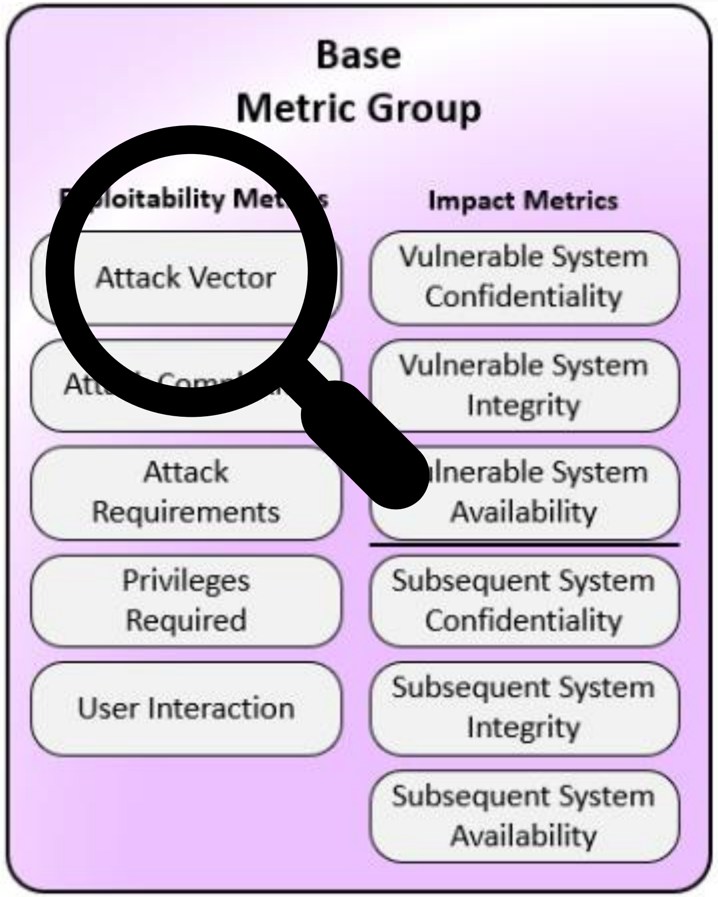


MacroVectors	Score
000000	10
000100	10
000001	9.9
010000	9.9
000010	9.8
001000	9.8
100000	9.8
010001	9.7
000101	9.6
000011	9.5
000020	9.5
001001	9.5
001010	9.5
010010	9.5
010100	9.5
011000	9.5
100001	9.5
110000	9.5
100010	9.4
100100	9.4
101000	9.4
000110	9.3
000200	9.3
001100	9.3
011001	9.3
200000	9.3

15M Combinations of Vectors → 270 Equivalence Sets → 0-10 Scores

Scoring Metrics Breakdown

CVSS 4 Base Metrics Group


Base
Metric Group
Exploitability Metrics
Impact Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability

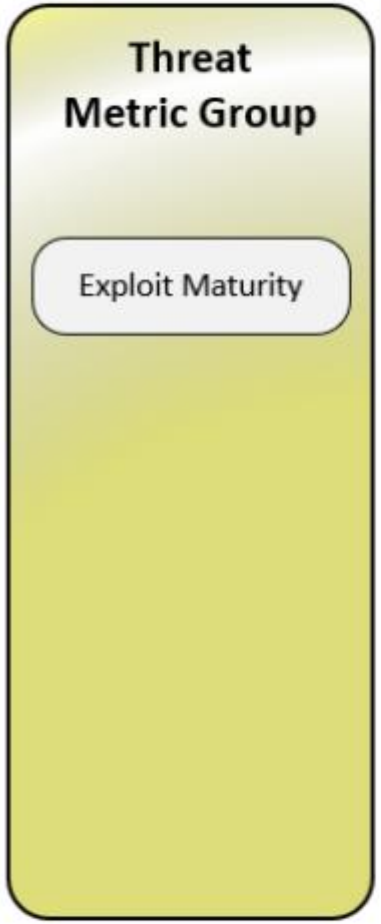
The **Attack Vector(AV)** metric describes how the vulnerability is exploited or the conditions an attacker needs to exploit the vulnerability. There are multiple categories for the attack vector, such as

1. Network => Internet facing or remotely
2. Adjacent => LAN, Bluetooth, NFC
3. Local => Console, Keyboard, or terminal (SSH)
4. Physical => Physically interact, writes a hacked bootloader

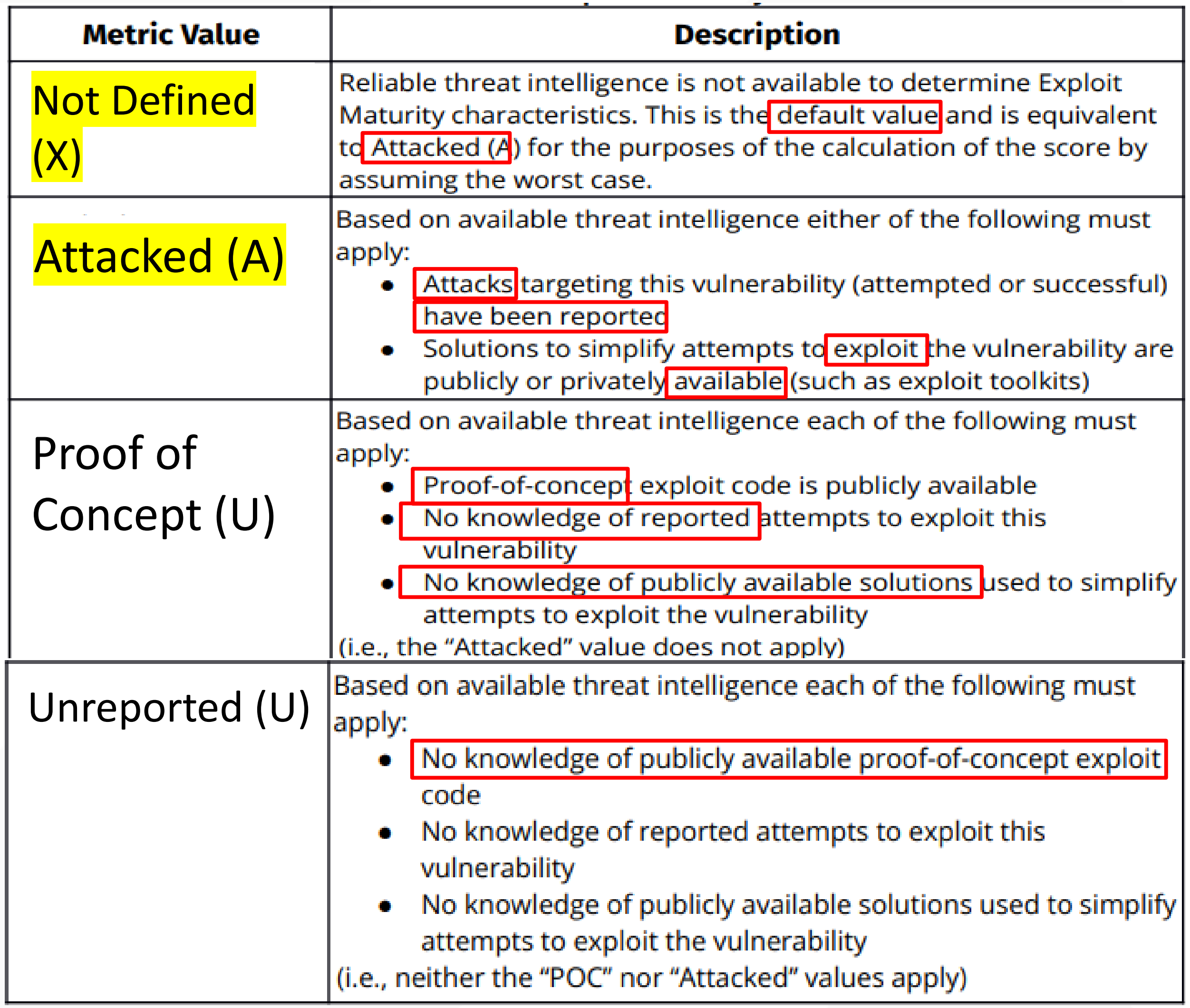
Provided by vulnerability researcher

CVSS 4 Threat Metrics Group

New



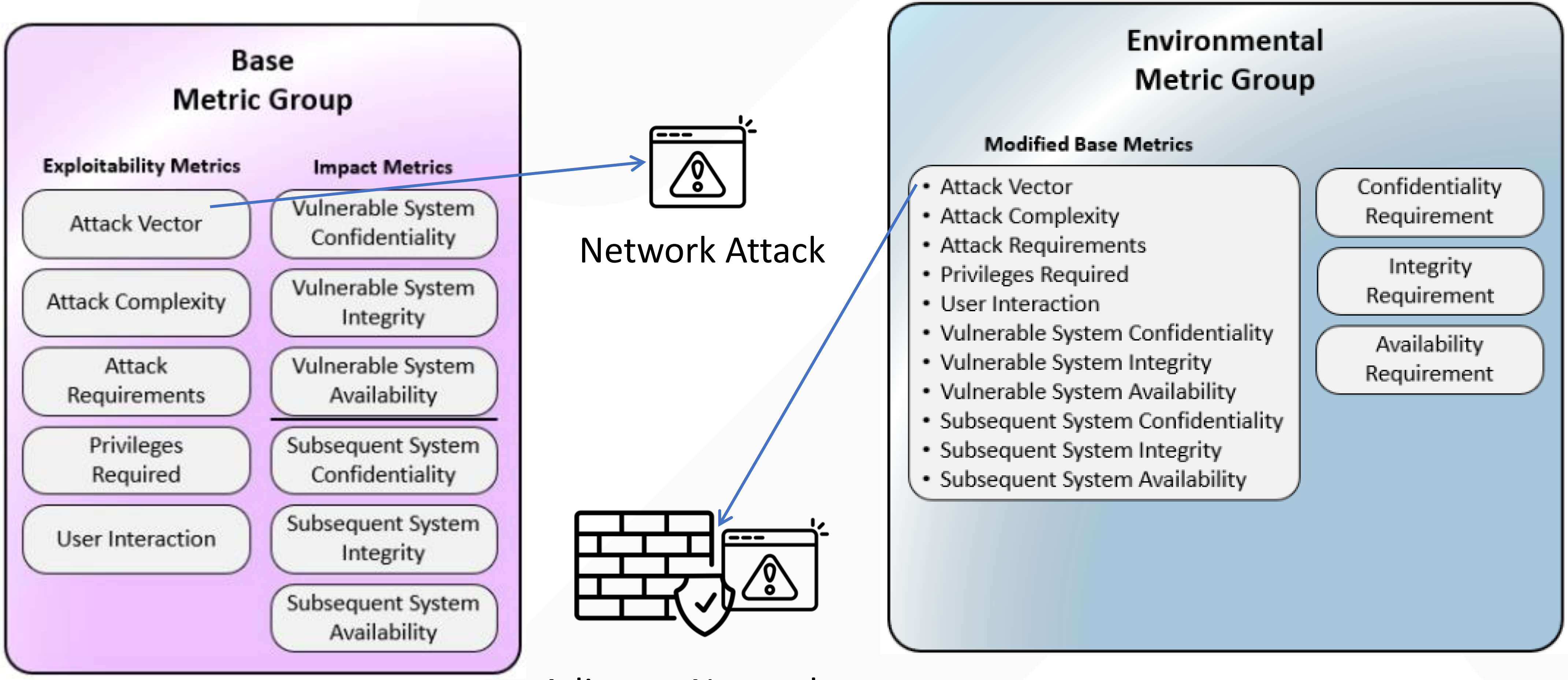
Provided by security **vendors**



Metric Value	Description
Not Defined (X)	Reliable threat intelligence is not available to determine Exploit Maturity characteristics. This is the default value and is equivalent to Attacked (A) for the purposes of the calculation of the score by assuming the worst case.
Attacked (A)	Based on available threat intelligence either of the following must apply: • Attacks targeting this vulnerability (attempted or successful) have been reported • Solutions to simplify attempts to exploit the vulnerability are publicly or privately available (such as exploit toolkits)
Proof of Concept (U)	Based on available threat intelligence each of the following must apply: • Proof-of-concept exploit code is publicly available • No knowledge of reported attempts to exploit this vulnerability • No knowledge of publicly available solutions used to simplify attempts to exploit the vulnerability (i.e., the "Attacked" value does not apply)
Unreported (U)	Based on available threat intelligence each of the following must apply: • No knowledge of publicly available proof-of-concept exploit code • No knowledge of reported attempts to exploit this vulnerability • No knowledge of publicly available solutions used to simplify attempts to exploit the vulnerability (i.e., neither the "POC" nor "Attacked" values apply)

https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf

CVSS 4 Environmental Metrics Group



Base Metric Group

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction

Impact Metrics

- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

Network Attack

Adjacent Network

Environmental Metric Group

Modified Base Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Provided by vulnerability **analyst**

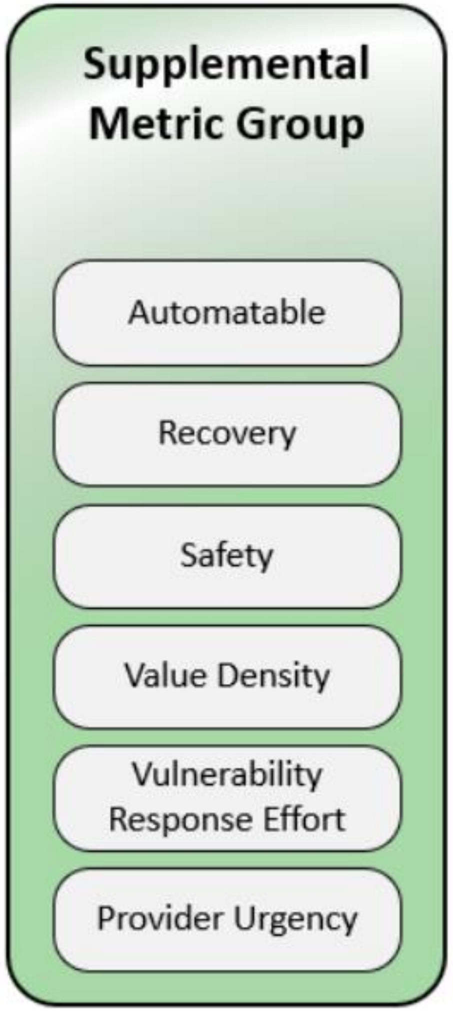
Assessed and filled out by the **user** based on their environment

CVSS 4 Supplemental Metrics Group

New

Optional.

Describe and measure additional extrinsic attributes of a vulnerability.



Supplemental Metric Group

Automatable

Recovery

Safety

Value Density

Vulnerability Response Effort

Provider Urgency

Provided by the provider

Metric	Description
Automatable (AU)	Can an attacker automate exploitation events for this vulnerability across multiple targets
Recovery (R)	The resilience of a system to recover services
Safety (S)	Impact on human or participant safety
Value Density (V)	Attacker will gain control over with a single exploitation event
Vulnerability Response Effort (RE)	How difficult it is for users to provide an initial response to the impact of vulnerabilities in their infrastructure
Provider Urgency (U)	Provider provides severity rating to user

CVSS-BTE Results

New

CVSS provided by discoverer / researcher

CVSS-B CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

10.0 / Critical

Exploit Maturity (E): Not Defined (X)
Use default value Attacked(A)

Threat Information provided by vendors

CVSS-BT CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:U

9.1 / Critical

Exploit Maturity (E): Unreported (U)

Environmental factors are considered and recalculated by the user

CVSS-BTE CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:U

7.7 / High

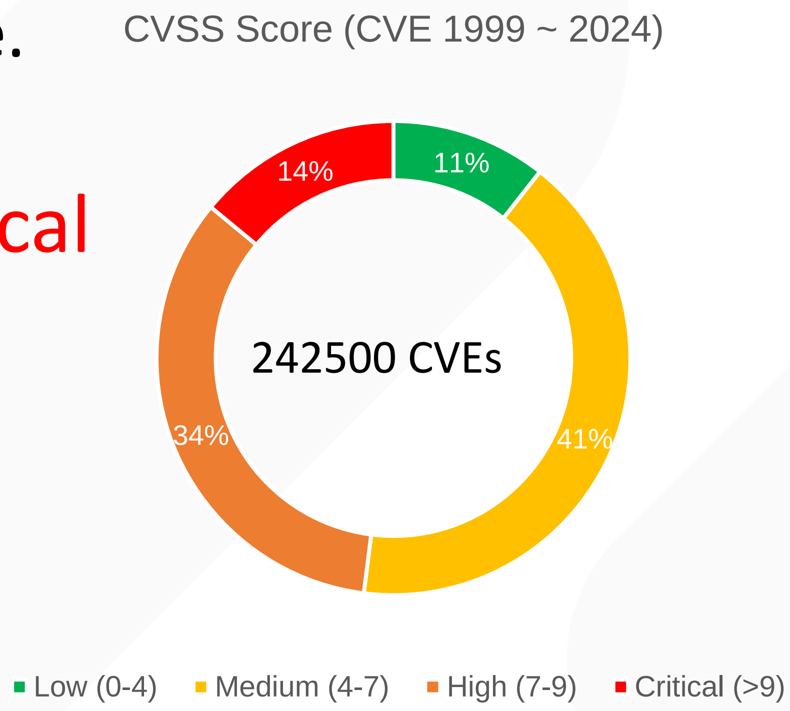
Attack Vector (AV): Adjacent Network
The vulnerable service is internal used only, not Internet facing

CVE CVSS scoring statistics (V2/V3)

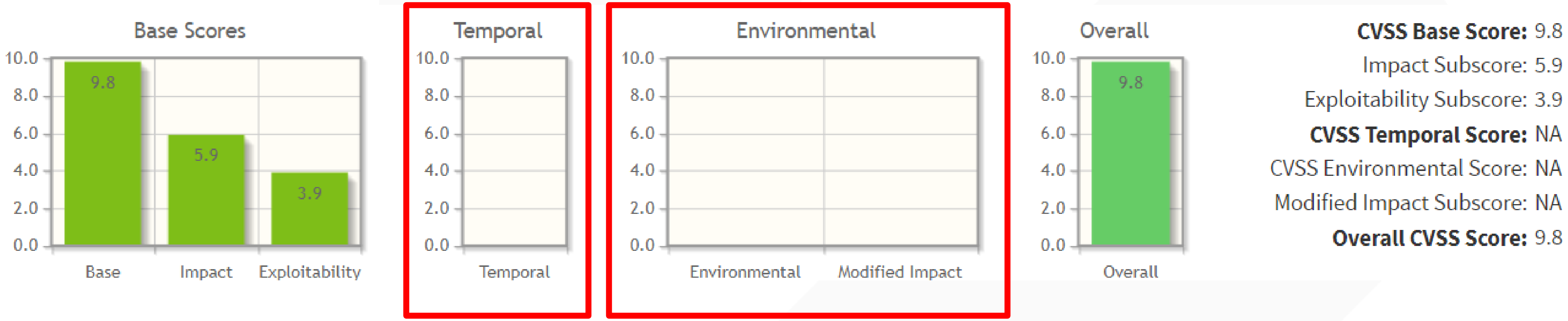
48% of CVEs have a CVSS score of 7 or above.

That means there are 116,402 High and Critical severity CVEs discovered.

13,482 CVEs in 2023 with CVSS scores over 7



CVSS 3.1 Usually, only the Base metrics are filled out.



CVSS Base Score: 9.8
Impact Subscore: 5.9
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.8

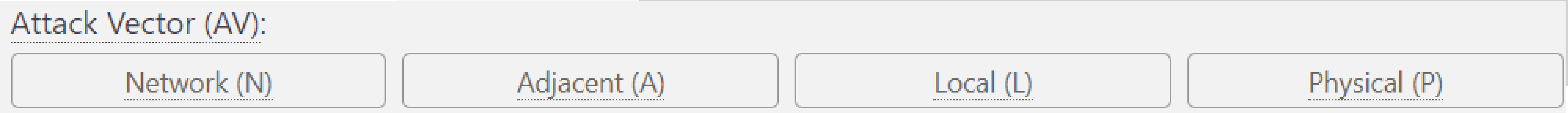
The Temporal parameters are provided by the security analyst,
And the Environmental parameters are filled out by the user based on the specific environment.

However, often both are left blank,
If left blank, it will be assumed under the worst-case scenario.

Case Study

Vulnerability Description - Exploitability Metrics -1

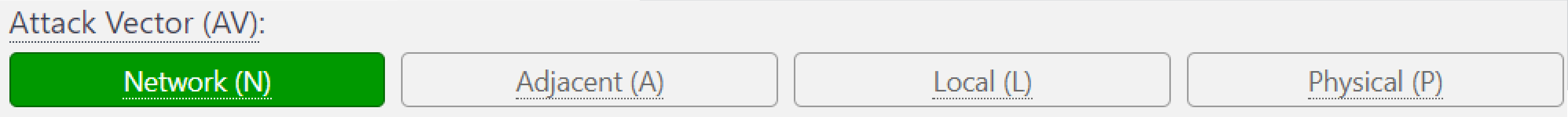
1. You are a web application developer working with security researchers on the security team.
2. Discover a vulnerability in your product.
3. After your investigation, it was found that the attack can be through the Internet


Attack Vector (AV):

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Vulnerability Description - Exploitability Metrics -1

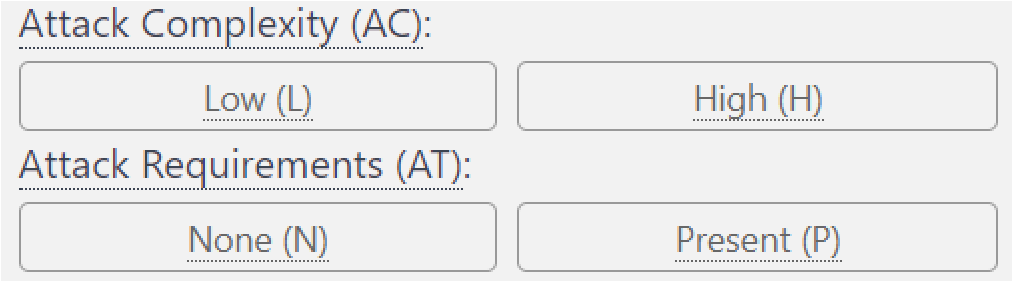
1. You are a web application developer working with security researchers on the security team.
2. Discover a vulnerability in your product.
3. After your investigation, it was found that the attack can be through the Internet


Attack Vector (AV):

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

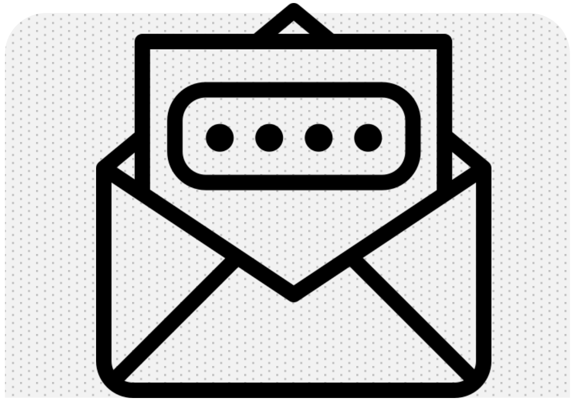
Vulnerability Description - Exploitability Metrics -2

4. No built-in security-enhancing mechanisms
5. The vulnerability occur by leveraging a specific plugin component



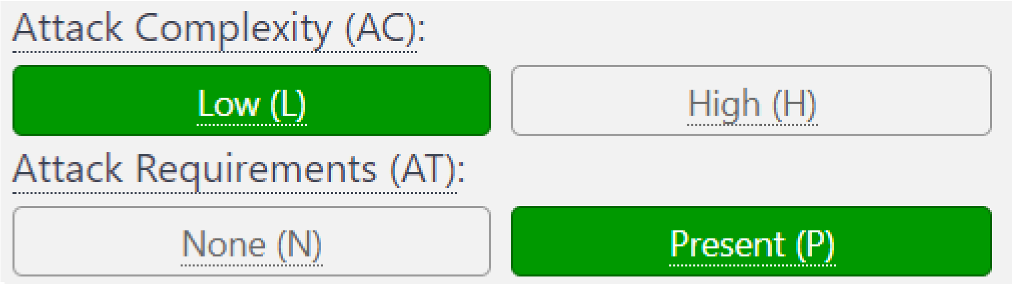
Attack Complexity (AC):

Attack Requirements (AT):



Vulnerability Description - Exploitability Metrics -2

4. No built-in security-enhancing mechanisms
5. The vulnerability occur by leveraging a specific plugin component



Attack Complexity (AC):

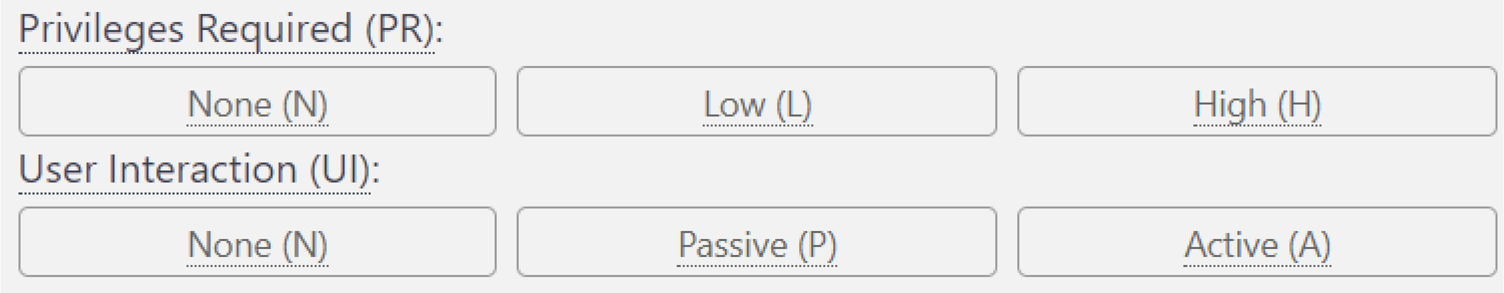
[✓ Low (L)] High (H)

Attack Requirements (AT):

None (N) [✓ Present (P)]

Vulnerability Description - Exploitability Metrics -3

6. The vulnerability can be exploited without user authentication
7. The attack does not require the use of any social engineering or user interaction



Privileges Required (PR):

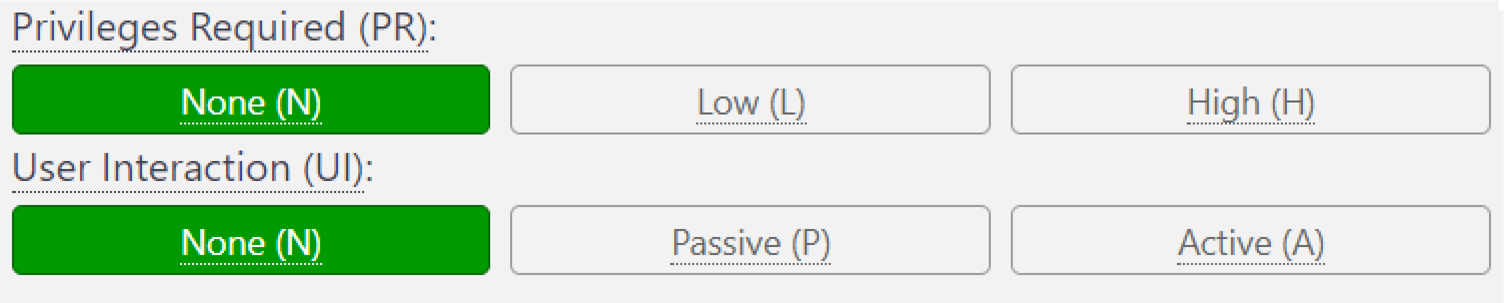
None (N)	Low (L)	High (H)

User Interaction (UI):

None (N)	Passive (P)	Active (A)

Vulnerability Description - Exploitability Metrics -3

6. The vulnerability can be exploited without user authentication
7. The attack does not require the use of any social engineering or user interaction



Privileges Required (PR):

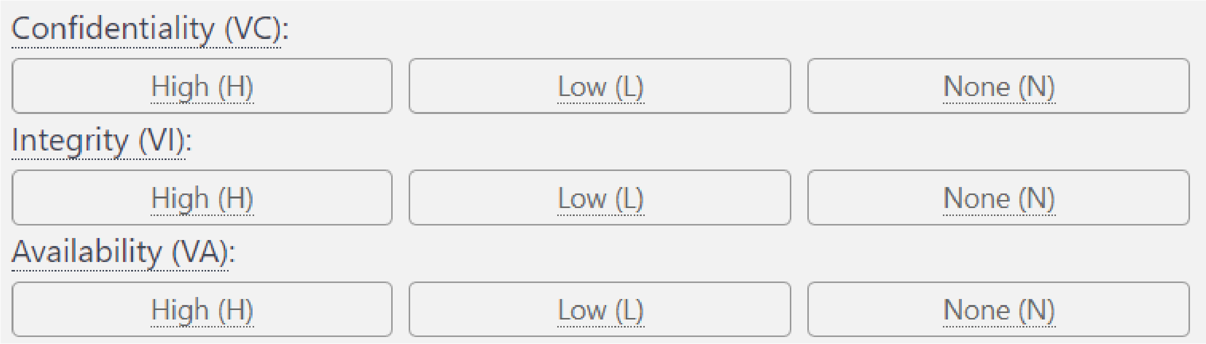
[✓ None (N)] Low (L) High (H)

User Interaction (UI):

[✓ None (N)] Passive (P) Active (A)

Vulnerability Description – Impact Metrics

1. If the attack is successful, the administrator password will be obtained by the attacker.
2. Cannot modification of system data
3. Affected systems will not lose availability



Confidentiality (VC):

High (H) | Low (L) | None (N)

Integrity (VI):

High (H) | Low (L) | None (N)

Availability (VA):

High (H) | Low (L) | None (N)

Confidentiality

- Data can only be accessed by authorized user

Integrity

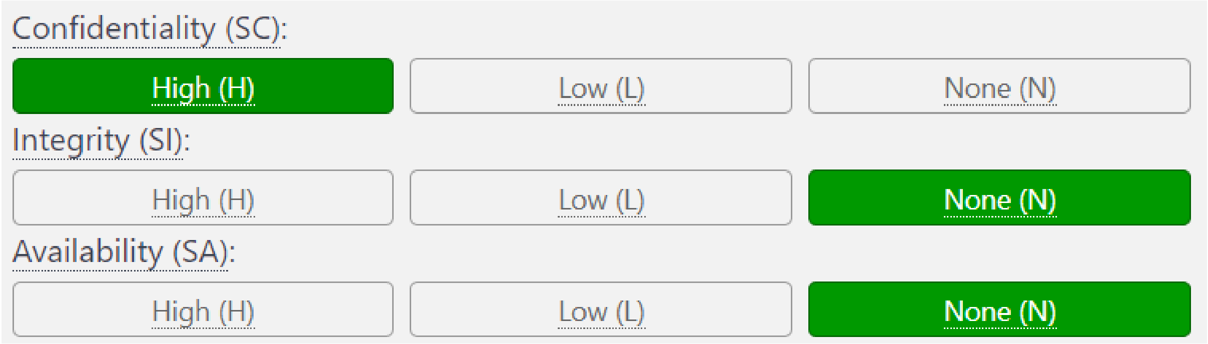
- Data is accurate, complete and trusted

Availability

- Systems are accessible

Vulnerability Description – Impact Metrics

1. If the attack is successful, the administrator password will be obtained by the attacker.
2. Cannot modification of system data
3. Affected systems will not lose availability



Confidentiality (SC):
[✓ High (H)] Low (L) None (N)

Integrity (SI):
High (H) Low (L) [✓ None (N)]

Availability (SA):
High (H) Low (L) [✓ None (N)]

Confidentiality

- Data can only be accessed by authorized user

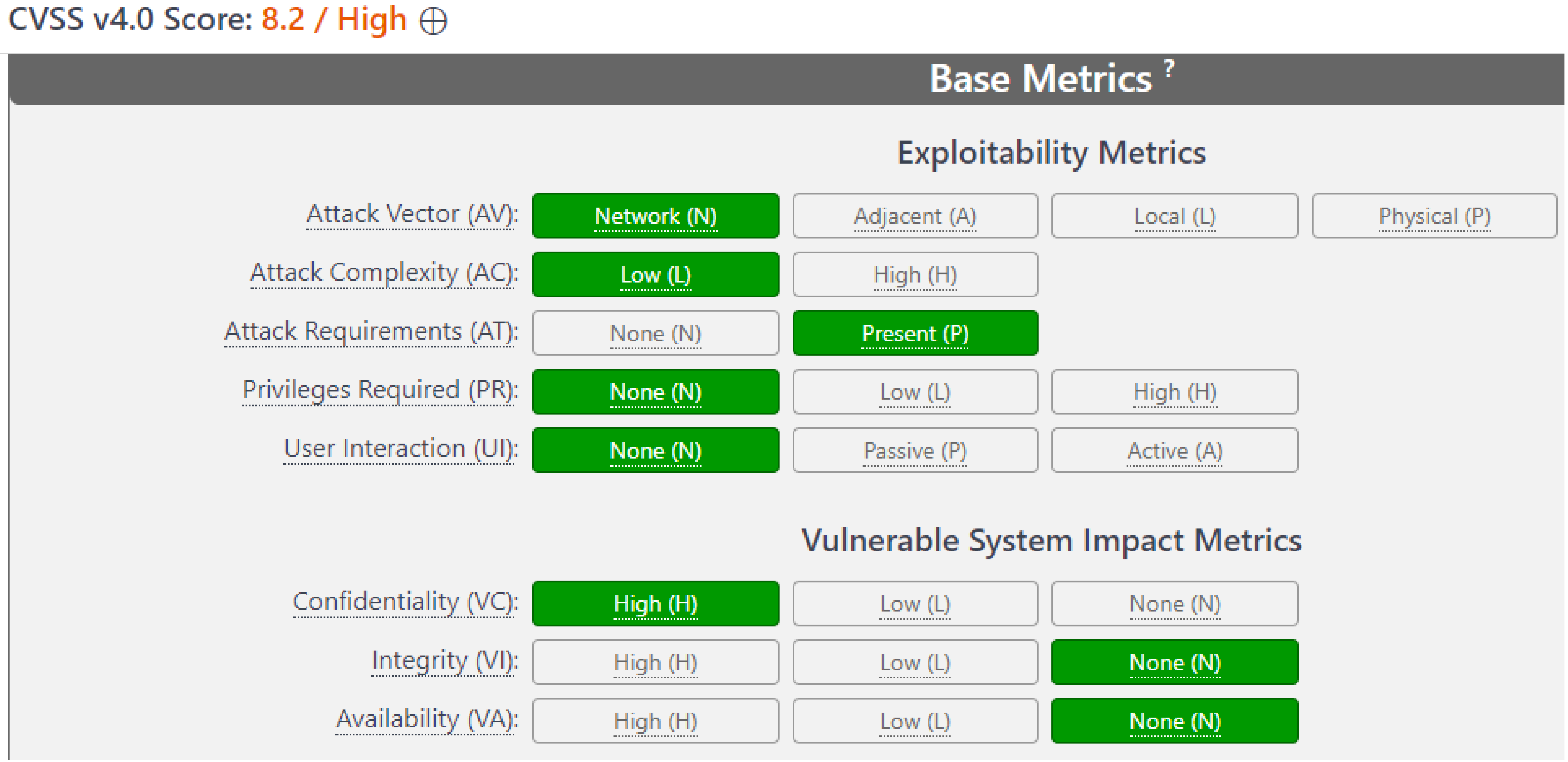
Integrity

- Data is accurate, complete and trusted

Availability

- Systems are accessible

Vulnerability Score Calculate



CVSS v4.0 Score: 8.2 / High

Base Metrics ?

Exploitability Metrics

Attack Vector (AV):	[✓ Network (N)]	Adjacent (A)	Local (L)	Physical (P)
Attack Complexity (AC):	[✓ Low (L)]	High (H)		
Attack Requirements (AT):	None (N)	[✓ Present (P)]		
Privileges Required (PR):	[✓ None (N)]	Low (L)	High (H)	
User Interaction (UI):	[✓ None (N)]	Passive (P)	Active (A)	

Vulnerable System Impact Metrics

Confidentiality (VC):	[✓ High (H)]	Low (L)	None (N)
Integrity (VI):	High (H)	Low (L)	[✓ None (N)]
Availability (VA):	High (H)	Low (L)	[✓ None (N)]

https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Conclusion

Conclusion

Changes

- The limitations
- CVSS V4 added new vectors and group

Calculate

- How to measure vulnerabilities
- CVSS Calculator

Metric Group

- CVSS-B,CVSS-BT,CVSS-BTE
- CVSS it not just the Base score

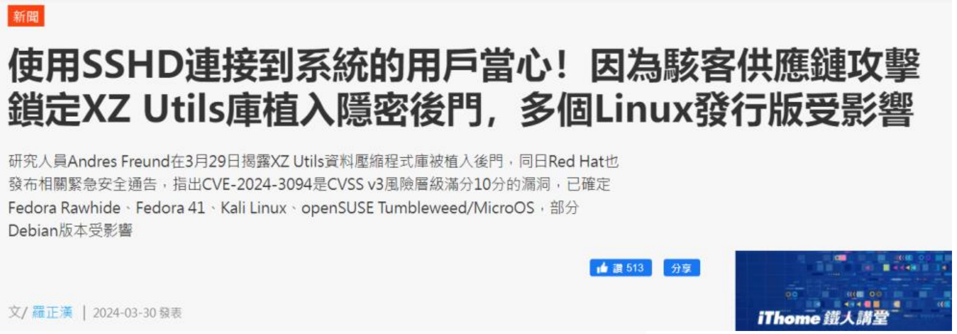
Threat Metrics and Environmental Metrics

XZ-Utils Supply Chain Backdoor Vulnerability (XZBot)
CVE-2024-3094

# CVSS 3.1

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Score: 10.0 Critical



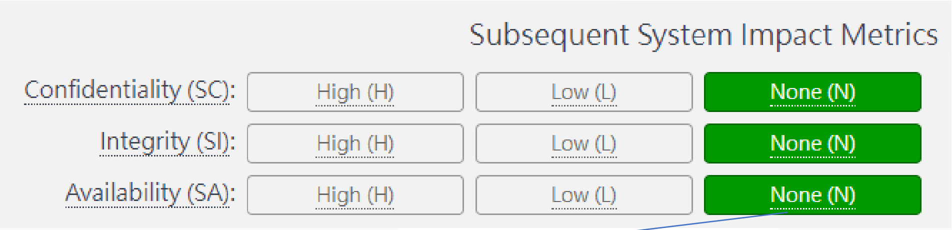
新聞

使用SSHD連接到系統的用戶當心！因為駭客供應鏈攻擊鎖定XZ Utils庫植入隱密後門，多個Linux發行版受影響

研究人員Andres Freund在3月29日揭露XZ Utils資料壓縮程式庫被植入後門，同日Red Hat也發布相關緊急安全通告，指出CVE-2024-3094是CVSS v3風險層級滿分10分的漏洞，已確定Fedora Rawhide、Fedora 41、Kali Linux、openSUSE Tumbleweed/MicroOS，部分Debian版本受影響

文/ 羅正漢 | 2024-03-30 發表

https://www.ithome.com.tw/news/162040



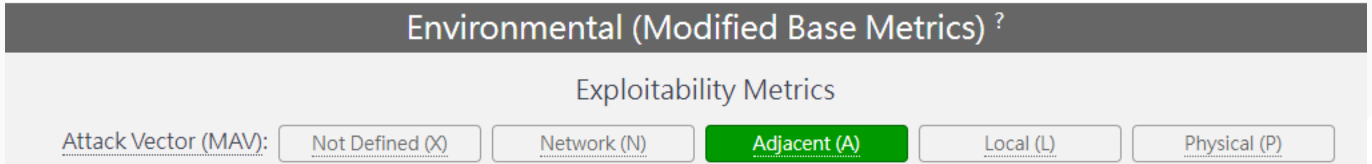
Subsequent System Impact Metrics

Confidentiality (SC): High (H) Low (L) [✓ None (N)]
Integrity (SI): High (H) Low (L) [✓ None (N)]
Availability (SA): High (H) Low (L) [✓ None (N)]

# CVSS 4.0

CVSS-B: 9.3 Critical

Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N



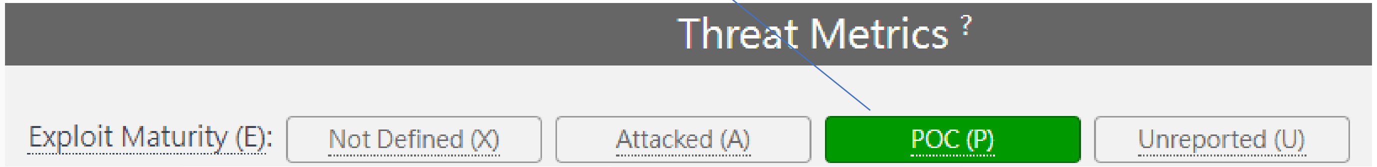
Environmental (Modified Base Metrics) ?

Exploitability Metrics

Attack Vector (MAV): Not Defined (X) Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

CVSS-BTE: 7.4 High

Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/MAV:A



Threat Metrics ?

Exploit Maturity (E): Not Defined (X) Attacked (A) [✓ POC (P)] Unreported (U)

Environmental Metrics
(Modified Base Metrics)

Wireless RF Insulin Pumps

#CVSS3.1

Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

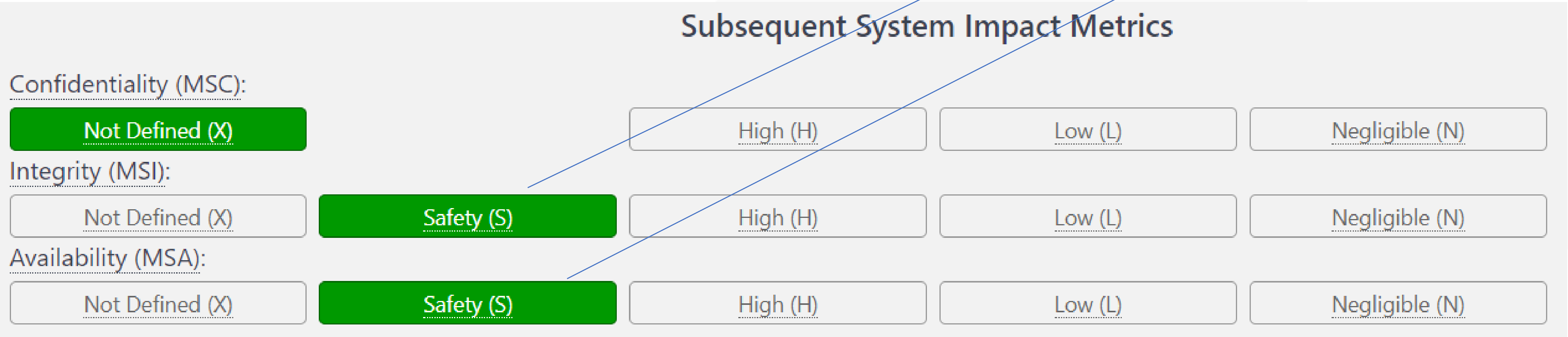
Score: 8.8 High

#CVSS4.0

Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/MAV:A/MAC:L/MPR:N/MUI:N/MVC:H/MVI:H/MVA:H/MSI:S/MSA:S

CVSS-BTE Score: 9.3 Critical

https://www.medtronicdiabetes.com/
CVE-2019-10964



Subsequent System Impact Metrics

Confidentiality (MSC):
[✓ Not Defined (X)] High (H) Low (L) Negligible (N)

Integrity (MSI):
Not Defined (X) [✓ Safety (S)] High (H) Low (L) Negligible (N)

Availability (MSA):
Not Defined (X) [✓ Safety (S)] High (H) Low (L) Negligible (N)

Q&A Session

16:10pm - 16:15pm

感謝您參加講座， 掃描QR Code填寫問卷即可到Q106攤位上玩遊戲得好禮