black hat
EUROPE 2024
DECEMBER 11-12, 2024
BRIEFINGS

The CVSS Deception: How We've Been **Misled** on Vulnerability Severity

Speaker(s):

Syed Islam & Ankur Sand

Agenda: Details

Agenda

- Introduction
- Vulnerability Management & CVSS
- Six Challenges in CVSS Utilization
  - Recommendations & Guidance
- Future Directions
- Key Takeaways

Who We Are

J.P.Morgan

Syed Islam

Principal Cybersecurity Architect

Cybersecurity and Technology Controls

https://syed-islam.github.io/

Ankur Sand

Vice President- Cybersecurity Operations Center

(Vulnerability Management Response)

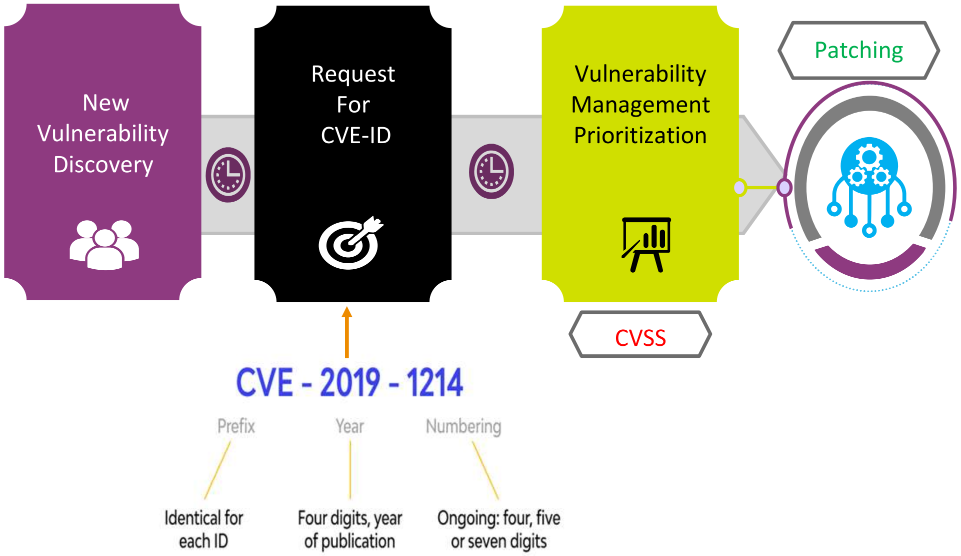
https://www.linkedin.com/in/ankur-s-14323a8/

Vulnerability Management
&
Common Vulnerability Scoring System (CVSS)

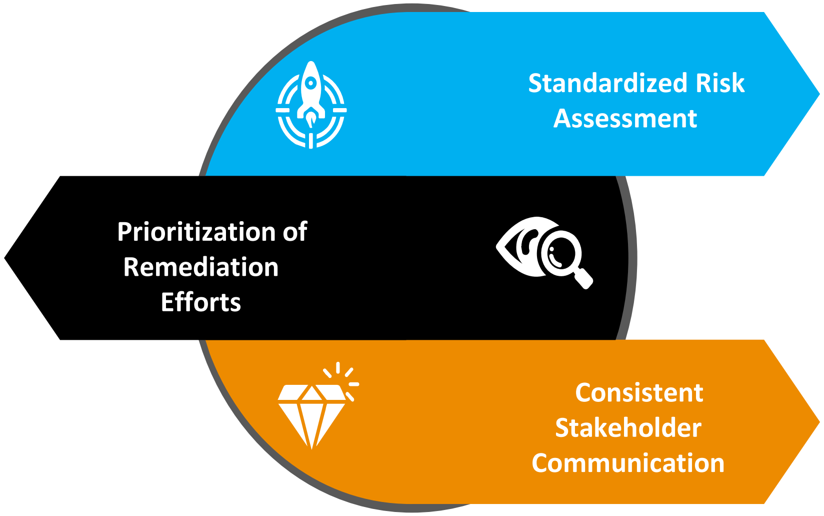
Vulnerability Management & CVSS - CVE Lifecycle & Impact

Vulnerability Lifecycle and CVSS for Severity Assessment

Lifecycle of a Vulnerability


New Vulnerability Discovery
Request For CVE-ID
Vulnerability Management Prioritization
Patching
CVSS
CVE - 2019 - 1214
Prefix
Year
Numbering
Identical for each ID
Four digits, year of publication
Ongoing: four, five or seven digits

Role of CVSS in Vulnerability Assessment

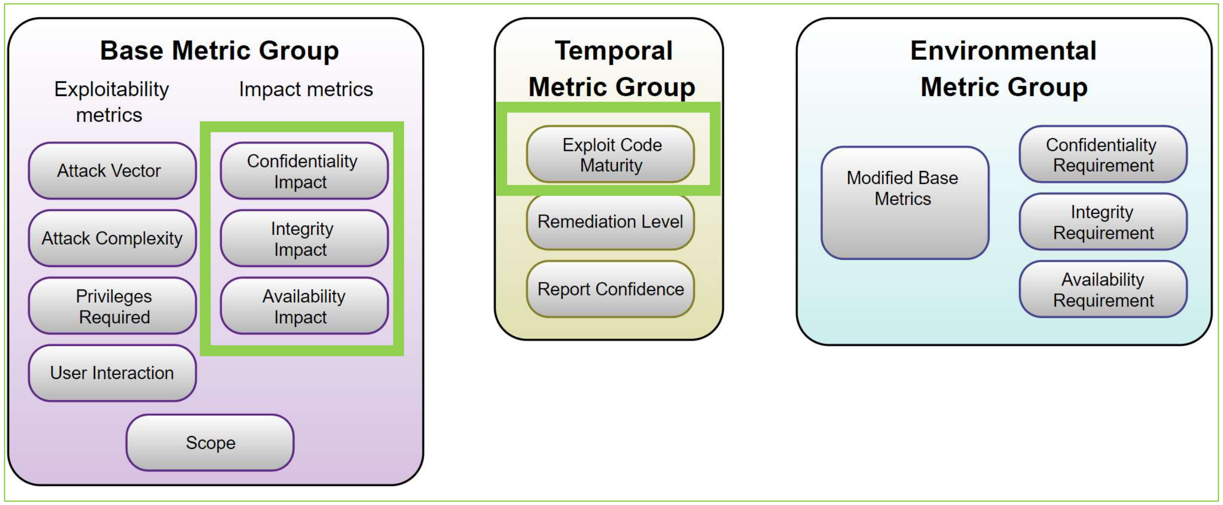

Standardized Risk Assessment
Prioritization of Remediation Efforts
Consistent Stakeholder Communication

https://www.wallarm.com/what/common-vulnerabilities-and-exposures-cve

Vulnerability Management & CVSS - Details

CVSS 3.0/ 3.1 Metrics and Severity Scale

CVSS Scoring Metrics Details



Base Metric Group

Exploitability metrics

Attack Vector

Attack Complexity

Privileges Required

User Interaction

Impact metrics

Confidentiality Impact

Integrity Impact

Availability Impact

Scope

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Source: https://www.first.org/cvss/v3.1/specification-document

CVSS Severity Levels

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

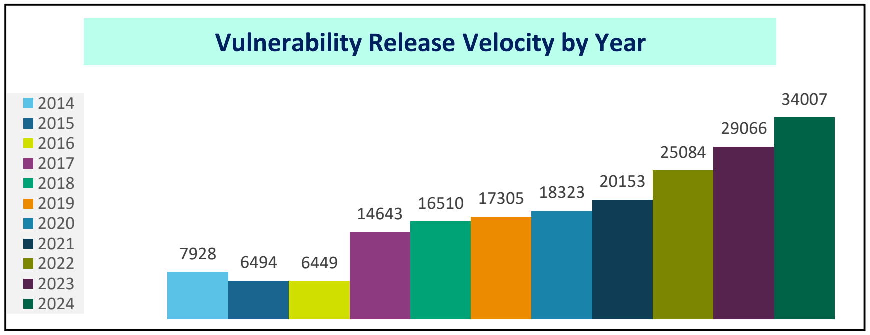
Vulnerability Management & CVSS - Trends

Vulnerability Disclosure Trends

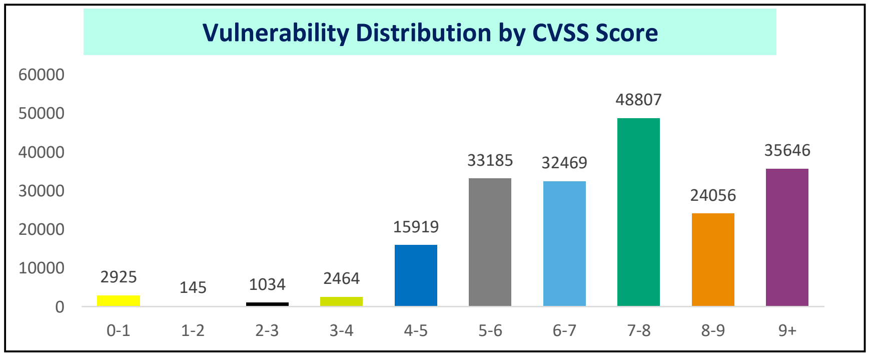
Annual CVE disclosures rate trending up by **~20%**
18% of CVEs rated **critical** (CVSS score of 9+).

Most common vulnerability types:

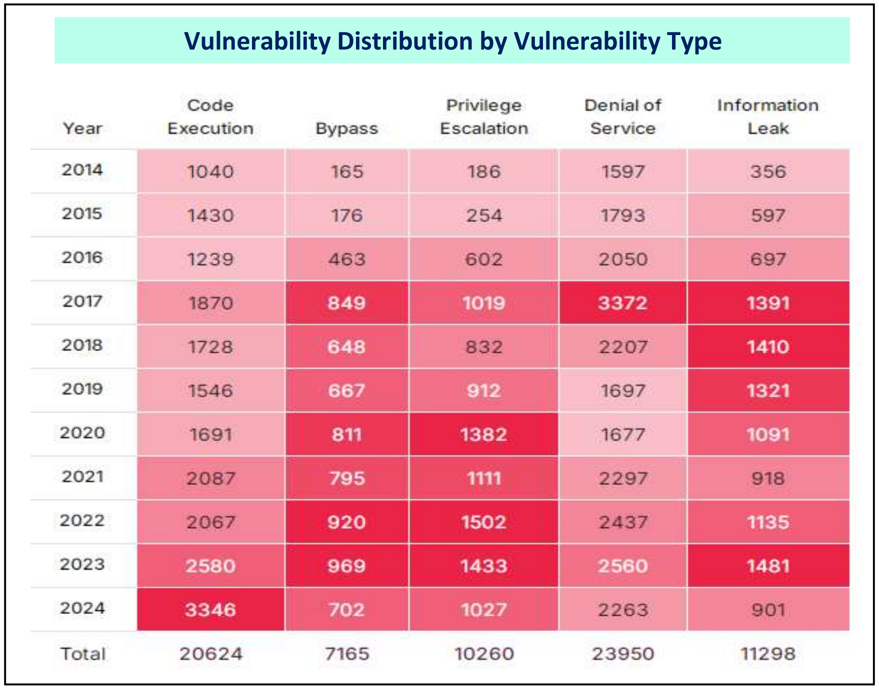
- Denial of Service - 32%
- Code Execution - 28%



Vulnerability Release Velocity by Year



Vulnerability Distribution by CVSS Score



Vulnerability Distribution by Vulnerability Type

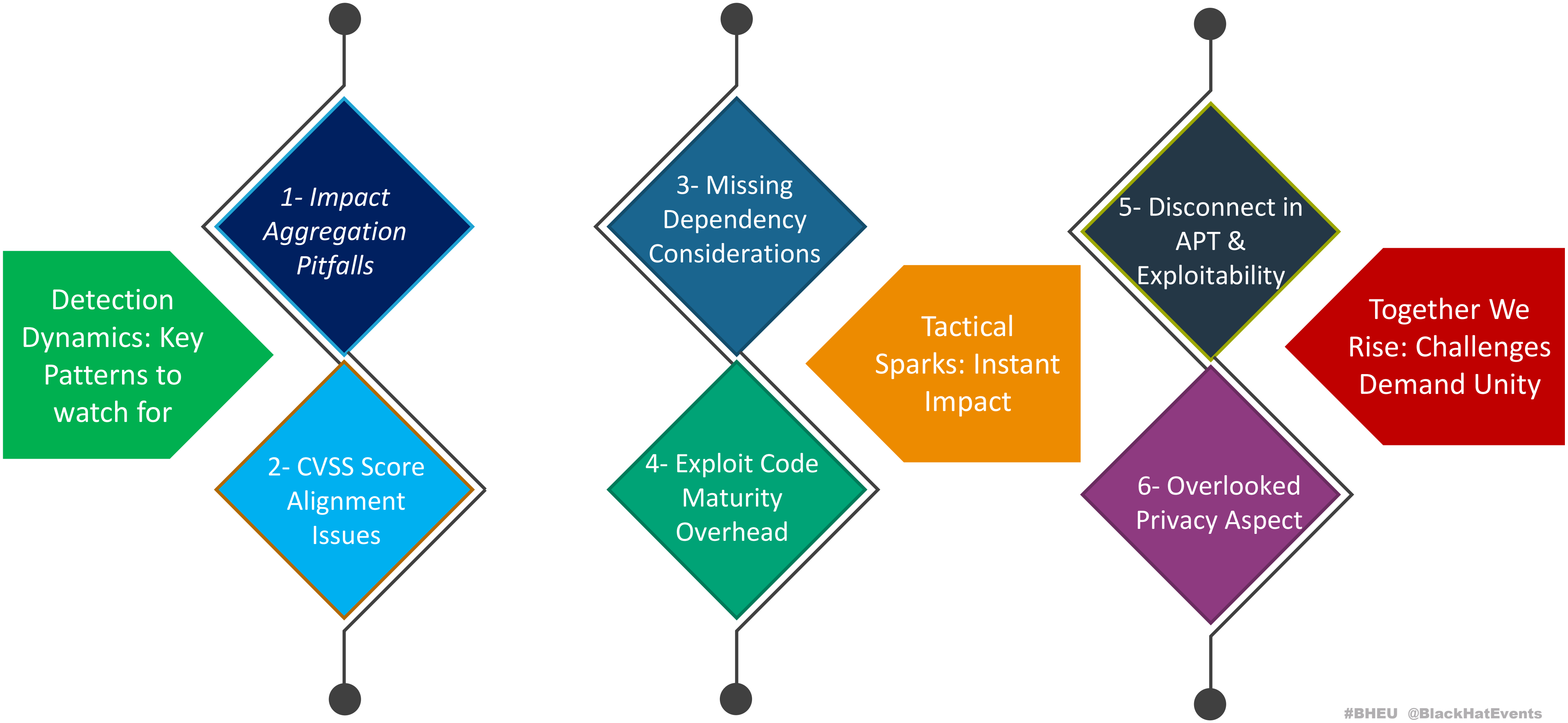
Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	1040	165	186	1597	356
2015	1430	176	254	1793	597
2016	1239	463	602	2050	697
2017	1870	849	1019	3372	1391
2018	1728	648	832	2207	1410
2019	1546	667	912	1697	1321
2020	1691	811	1382	1677	1091
2021	2087	795	1111	2297	918
2022	2067	920	1502	2437	1135
2023	2580	969	1433	2560	1481
2024	3346	702	1027	2263	901
Total	20624	7165	10260	23950	11298

Source: https://www.cvedetails.com/

Operational Challenges with CVSS

Operational Roadblocks in CVSS - Challenges

CVSS Adoptions- Operational Challenges with CVSS 3.0/3.1



Detection Dynamics: Key Patterns to watch for

1- Impact Aggregation Pitfalls

2- CVSS Score Alignment Issues

3- Missing Dependency Considerations

4- Exploit Code Maturity Overhead

Tactical Sparks: Instant Impact

5- Disconnect in APT & Exploitability

6- Overlooked Privacy Aspect

Together We Rise: Challenges Demand Unity

Detection Dynamics: Key Patterns to Watch For

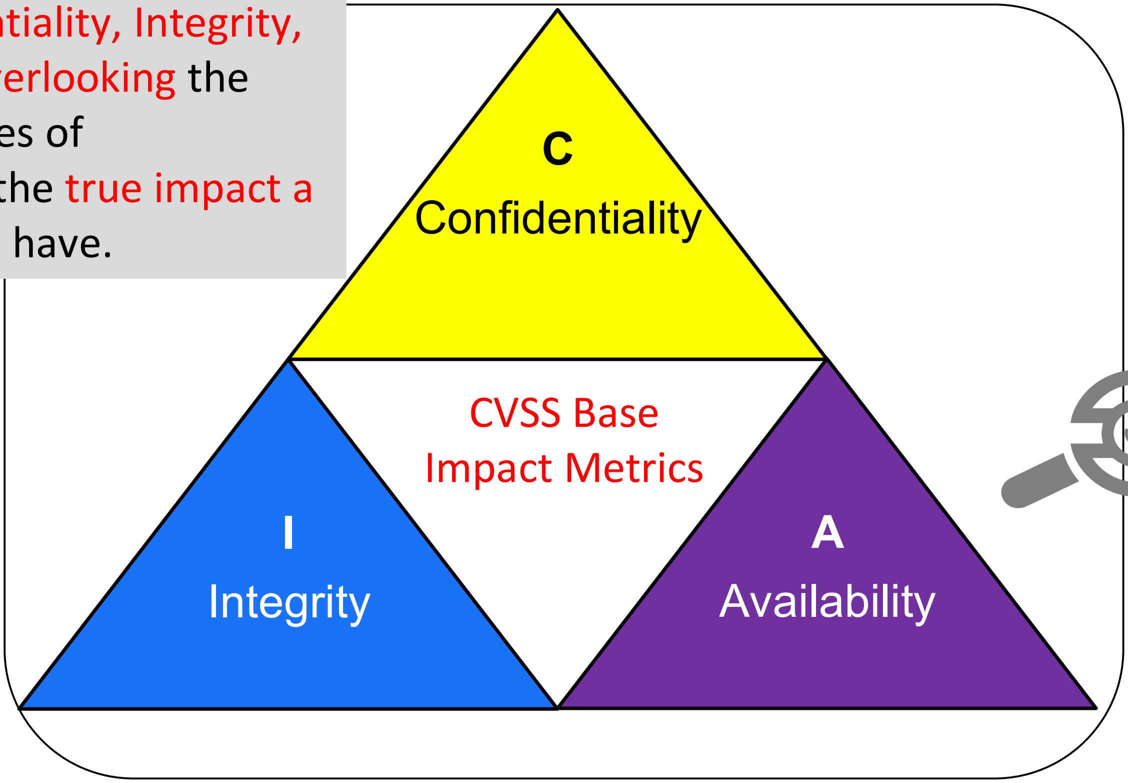
1- Aggregation Pitfalls

(Inability to express Vulnerability Severity using aggregation of CIA Metrics)

1 - Aggregation Pitfalls - Issue Details

CVSS -CIA Triad and Rating Scale with Numerical Weight

CVSS impact metrics give equal weight to Confidentiality, Integrity, and Availability, overlooking the unique risk priorities of organizations and the true impact a vulnerability might have.

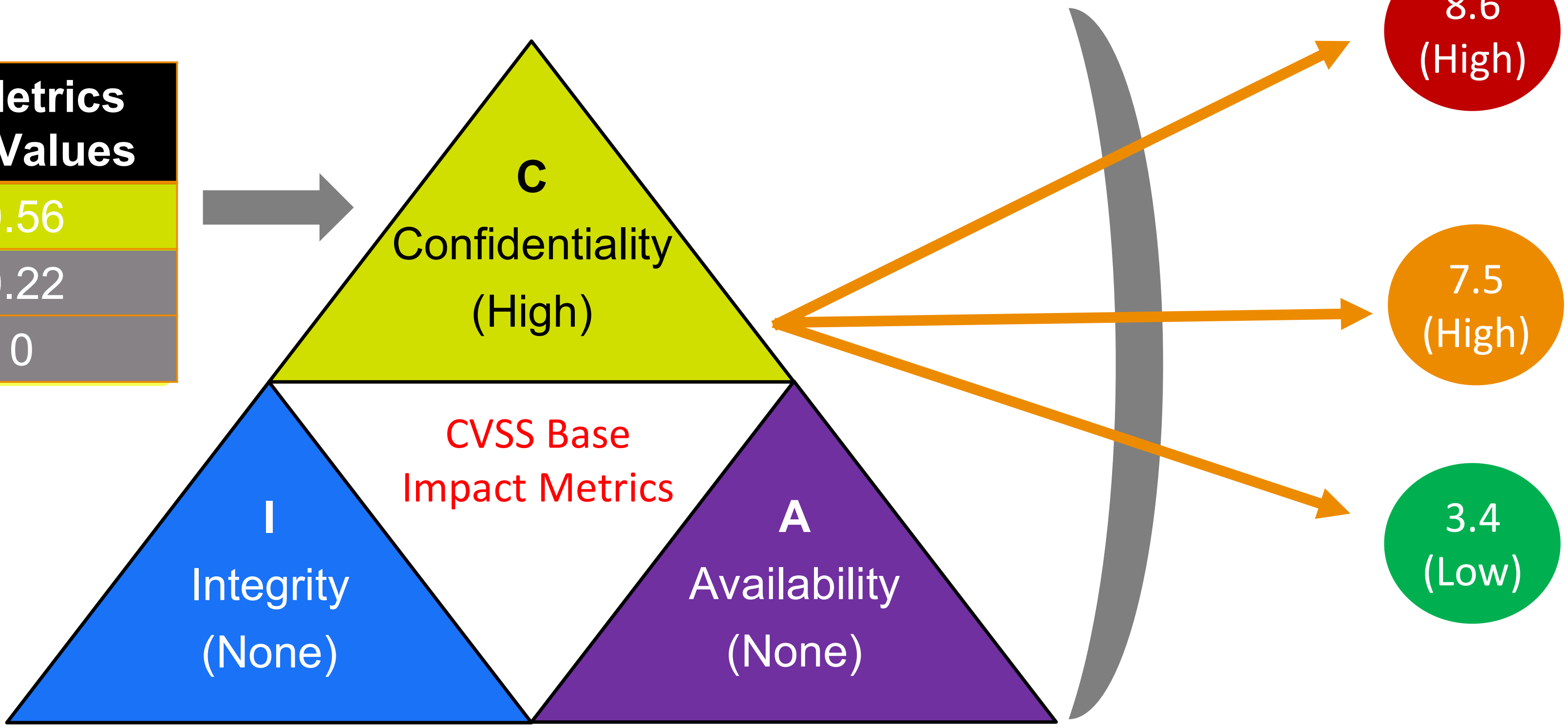


C,I,A Impact- Metrics and Numerical Values	
High	0.56
Low	0.22
None	0

1 - Aggregation Pitfalls - Issue Details

CIA Triad and CVSS Outcome (When One Value as High others as None)

C,I,A Impact- Metrics and Numerical Values	
High	0.56
Low	0.22
None	0



1 - Aggregation Pitfalls – Case Study

Case Study- Real-World Examples showing Unauthorized DDos attack against Critical Business Services

Source: https://tvcidade10.com.br/wp-content/uploads/2023/02/691913fc-d045-4d17-b804-4145d5f3a42d.jpg

Use case:

During the COVID-19 pandemic, CVE-2020-8187, a Citrix NetScaler DDoS vulnerability, was released and can be responsible for disrupting critical business applications that support remote work.

Exploitation Details: The attack is straightforward, requiring no user interaction or elevated privileges, and can be executed remotely.

Impact:
Severe
Business continuity Risk

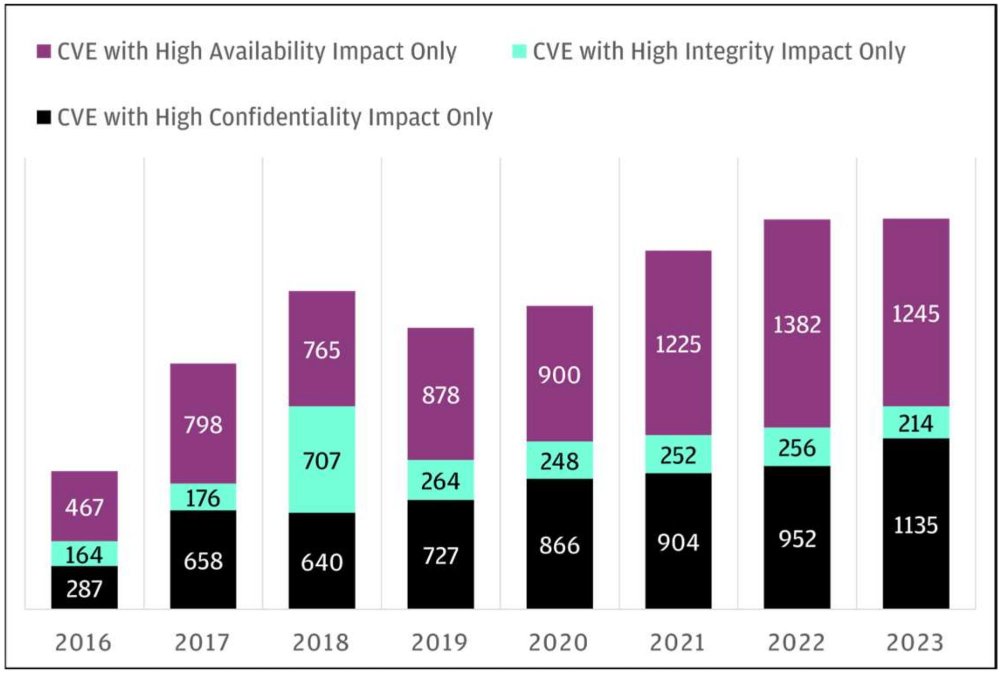
CVSS Rating
High

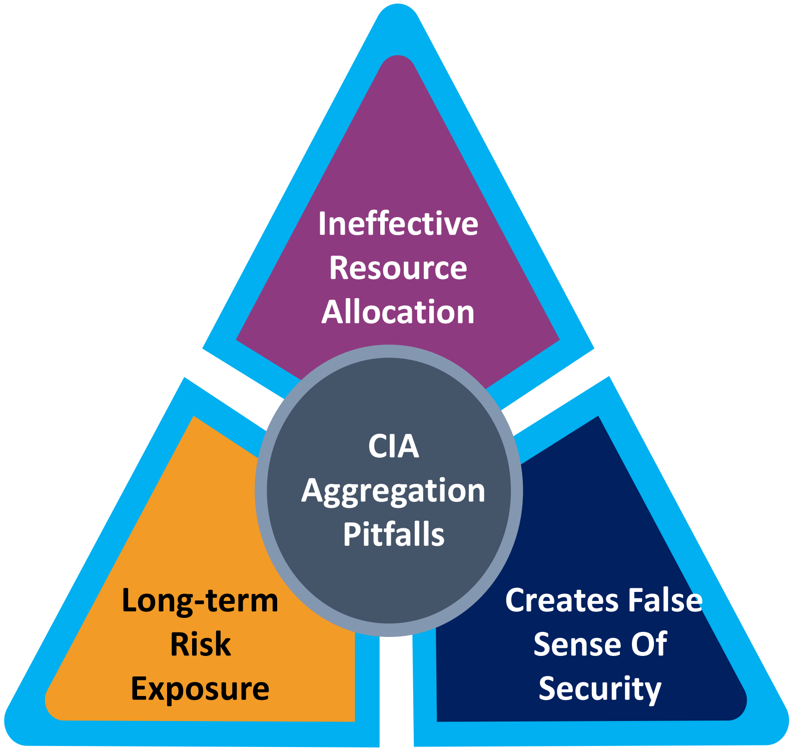
black hat EUROPE 2024

1- Aggregation Pitfalls - Statistics & Impact

Exposure and Impact Radius Covering Last Eight Years

Published CVEs that have *High* impact on only *one* Impact Metric and no impact on others.

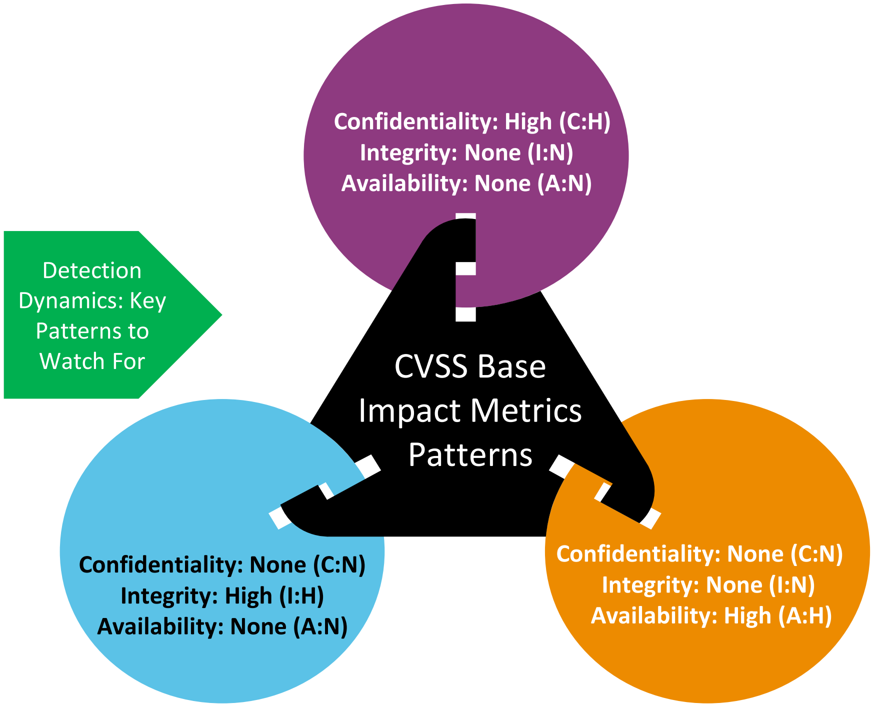




Ineffective Resource Allocation
CIA Aggregation Pitfalls
Long-term Risk Exposure
Creates False Sense Of Security

1- Aggregation Pitfalls – Detection Patterns

Recognizing Current Challenges and Providing Strategic Recommendations


Detection Dynamics: Key Patterns to Watch For
CVSS Base Impact Metrics Patterns
Confidentiality: High (C:H)
Integrity: None (I:N)
Availability: None (A:N)
Confidentiality: None (C:N)
Integrity: High (I:H)
Availability: None (A:N)
Confidentiality: None (C:N)
Integrity: None (I:N)
Availability: High (A:H)

Challenge Awareness:

- Aggregation of CIA impact metrics can **underrate** vulnerabilities that severely affect only one attribute, potentially delaying remediation efforts.
- **High volumes** of vulnerabilities lead organizations to prioritize by severity, risking prolonged risk exposures.

Recommendations:

- Develop capabilities to **incorporate CVSS vectors with a single CIA element rated as High and others as None** into vulnerability assessments, focusing on public-facing assets that support critical business services.

Detection Dynamics: Key Patterns to Watch For

2- CVSS Score Alignment Issues

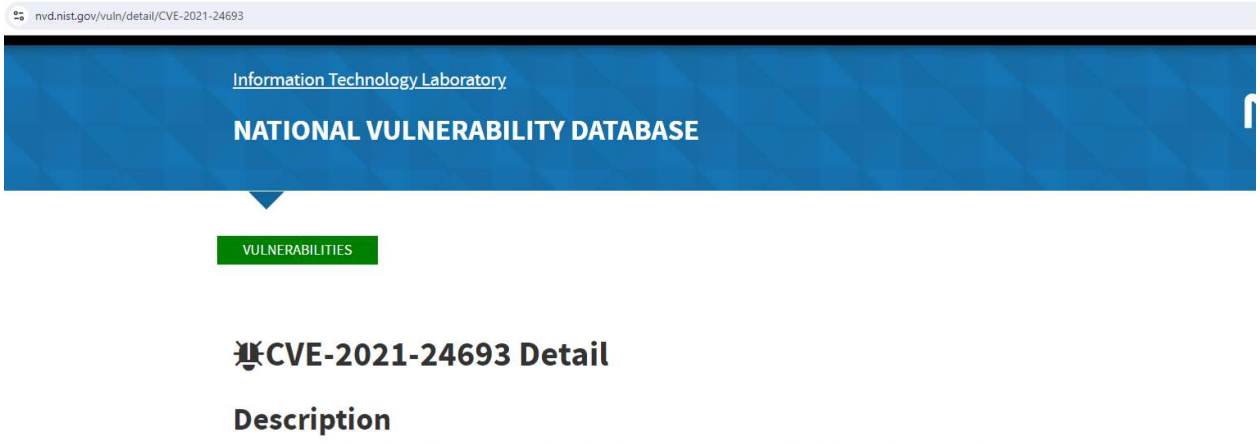
2 - CVSS Score Alignment Issues - Details

CVSS Score Alignment Issues

- **Scoring Discrepancy:** A rounding error in CVSS 3.0/ 3.1 causes a slight difference between Base and Environmental scores.
- **Input Vector Impact:** The specific input vector results in a Base score of 9.0 and an Environmental score of 9.1.
- **Framework Inconsistency:** Although the difference is minor (0.1 or 1%), it highlights a potential inconsistency within the CVSS framework.

2 - CVSS Score Alignment Issues - Case Study

Case Study- Real-World Examples showing CVSS Score Alignment Issue



nvd.nist.gov/vuln/detail/CVE-2021-24693

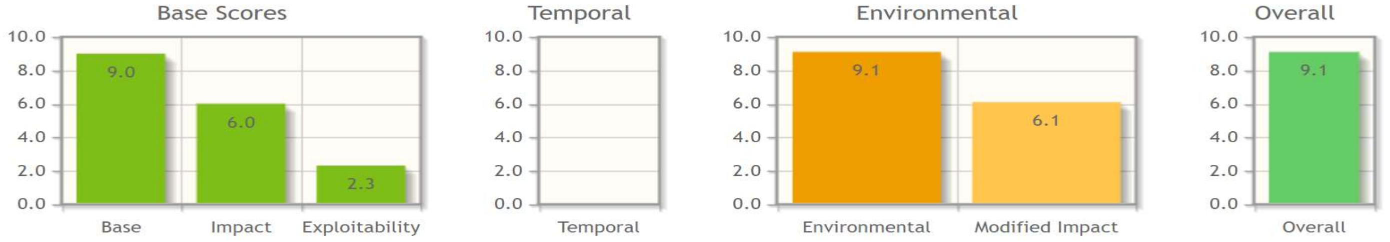
Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2021-24693 Detail

Description



CVSS Base Score: 9.0
Impact Subscore: 6.0
Exploitability Subscore: 2.3
CVSS Temporal Score: NA
CVSS Environmental Score: 9.1
Modified Impact Subscore: 6.1
Overall CVSS Score: 9.1

Show Equations

Detection Dynamics: Key Patterns to Watch For

CVSS v3.1 Vector

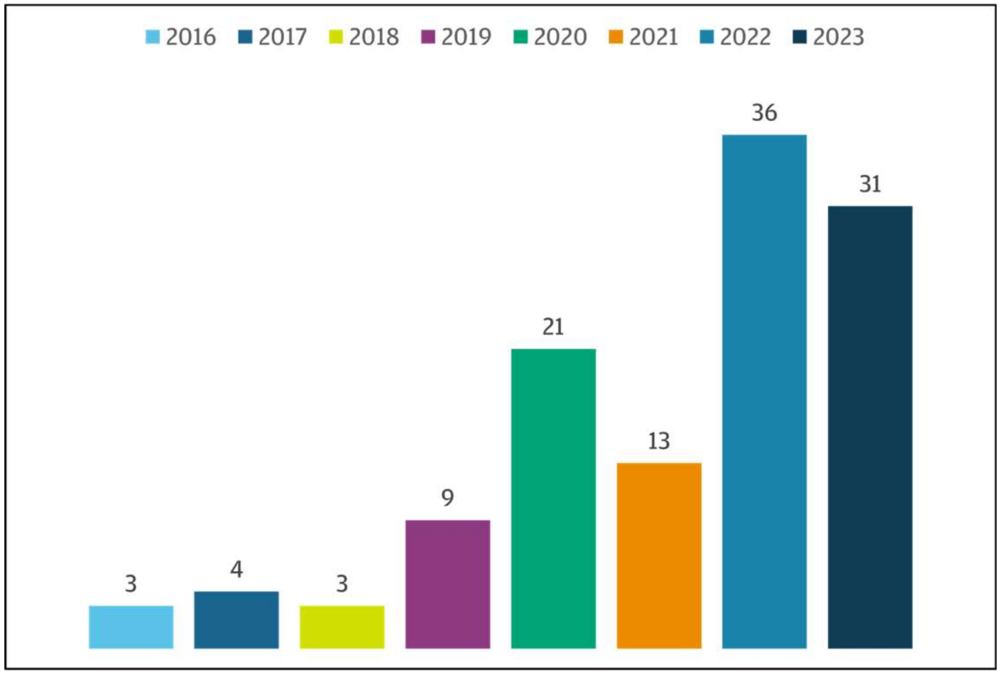
AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:L/MUI:R/MS:C/MC:X/MI:X/MA:X

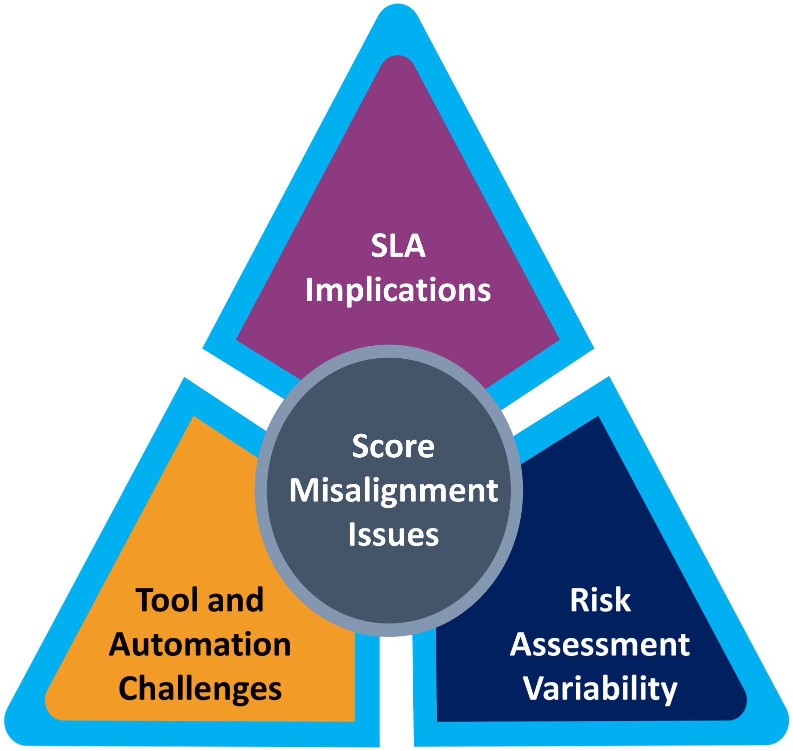
Source: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

2 - CVSS Score Alignment Issues - Statistics & Impact

CVEs with Mismatch Condition

Published CVEs that have
Base and Environmental Metric Mismatch





SLA Implications

Score Misalignment Issues

Tool and Automation Challenges

Risk Assessment Variability

2 - CVSS Score Alignment Issues - Detection Patterns

Recognizing Current Challenges and Providing Strategic Recommendations

Challenge Awareness:

- **Scoring Discrepancy:** A rounding error in CVSS 3.0/ 3.1 causes a slight difference between Base and Environmental scores.
- **Under Prioritization of Vulnerability:** The inconsistency in scoring can lead to lower prioritization if the it matches boundary condition

Recommendation:

- Develop capabilities to **identify pattern** AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H) and incorporate it into vulnerability assessments.
- Acknowledge and document as minor CVSS score discrepancy to ensures compliance and doesn't require any immediate actions.

3- Missing Dependency Considerations

Tactical Sparks: Instant Impact

3 - Missing Dependency Considerations - Issue Details

Pre- Requisite/Dependency and Vulnerability Exploitation

- **Network and Access Controls:** Configuration and Access Controls can significantly affect an attacker's ability to exploit a vulnerability

- **Configuration and Dependencies:** Exploits sometimes require specific setup or other software vulnerabilities

- **User Privileges:** Influence severity and potential impact

3 - Missing Dependency Considerations – Case Study

Case Study- Real-World Examples showing Missing Dependency Considerations

CVE-2023-4966 (Vendor Severity- Critical)

Malicious Threat Actor

Citrix NetScaler

Must Be Configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server

Mission Accomplished

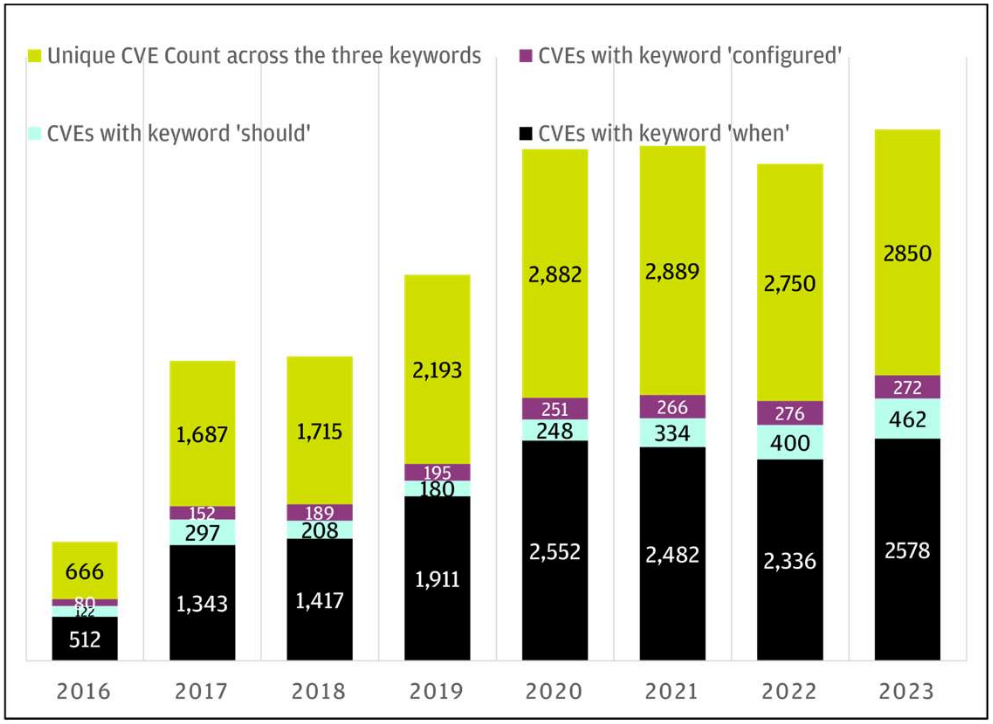
CVE- 2023-4966, a sensitive information disclosure vulnerability that allows an attacker to read large amounts of memory after the end of a buffer. Notably, that memory includes session tokens, which permits an attacker to impersonate another authenticated user

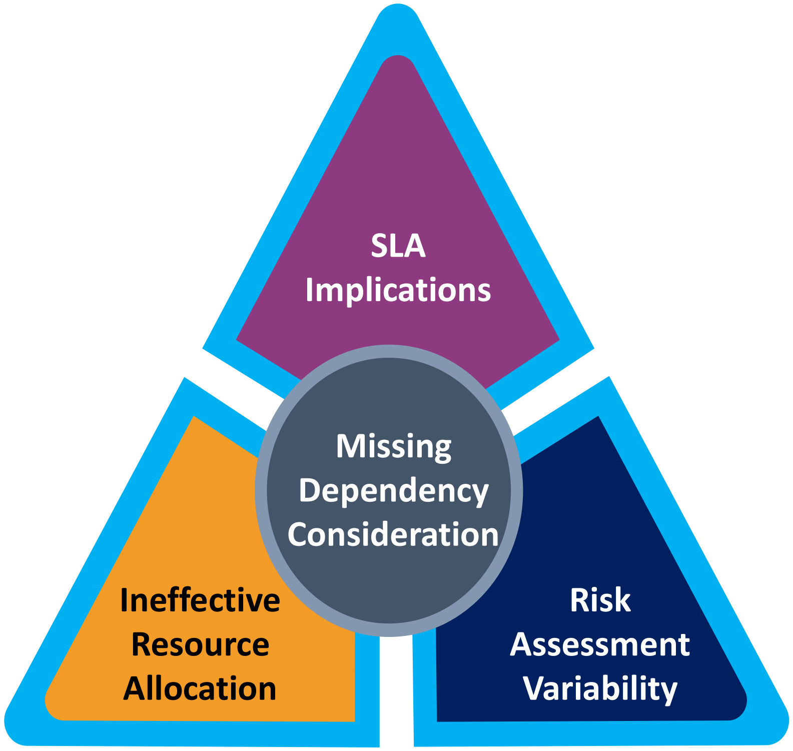
Source: https://support.citrix.com/s/article/CTX579459-netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967?language=en_US

3- Missing Dependency Considerations - Statistics & Impact

Exposure and Impact Radius

Published CVEs *with indicated Dependency / Environmental Requirements*




SLA Implications
Missing Dependency Consideration
Ineffective Resource Allocation
Risk Assessment Variability

3 - Missing Dependency Considerations – Detection

Recognizing Current Challenges and Providing Strategic Recommendations

Challenge Awareness:

- Lack of Pre-Requisite Environmental Considerations in CVSS.
- Approximately **11%** of vulnerabilities hold environmental dependencies
- Organizations struggle to prioritize vulnerabilities accurately, and continuous review against environmental changes adds complexity.

Recommendation:

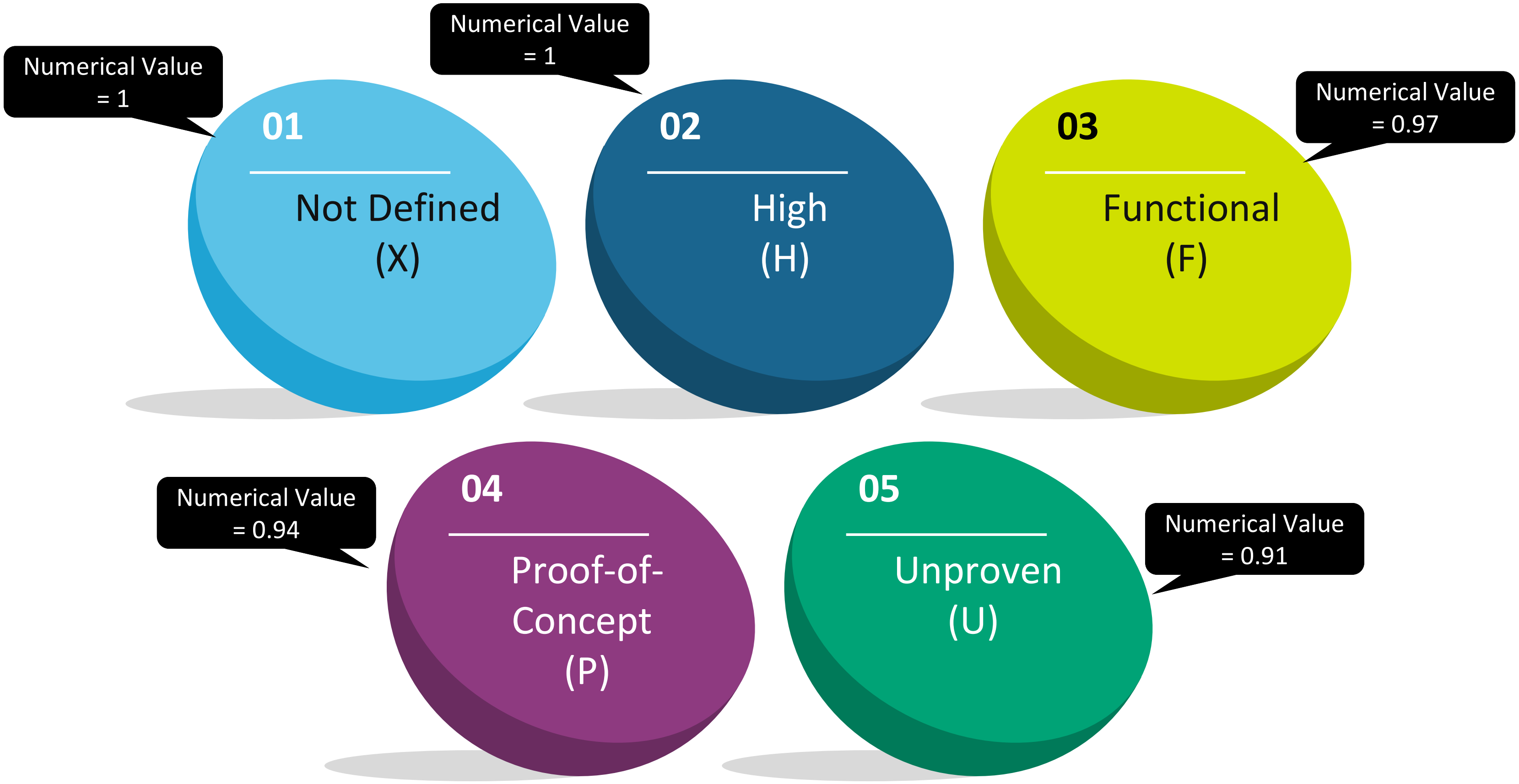
- Develop capabilities to **identify prerequisite** keywords ("when," "should," and "configured") and incorporate them into vulnerability assessments. With the progress in the LLM space we can now do this even better.

4- Exploit Code Maturity Overhead

Tactical Sparks: Instant Impact

4 - Exploit Code Maturity Overhead- Challenge Details

Exploit Code Maturity Metric Values



Numerical Value = 1

01 Not Defined (X)

Numerical Value = 1

02 High (H)

03 Functional (F)

Numerical Value = 0.97

Numerical Value = 0.94

04 Proof-of-Concept (P)

05 Unproven (U)

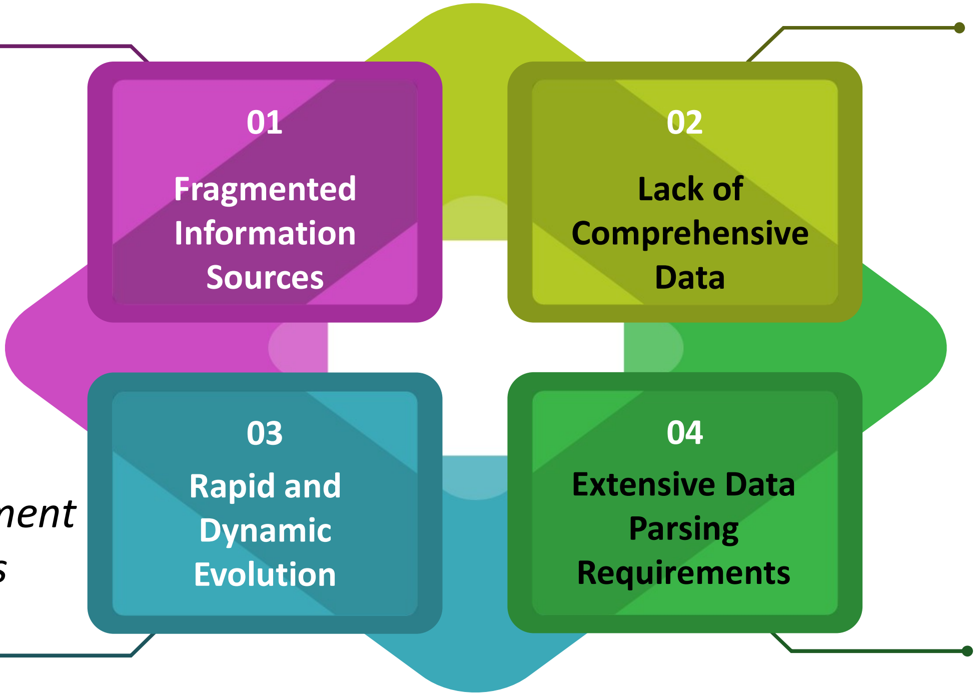
Numerical Value = 0.91

4 - Exploit Code Maturity Overhead- Challenge Details

Exploit Code Maturity Metric Monitoring Challenges

- *Scattered Sources*
- *Fragmentation Issue*
- *Incomplete Lifecycle Coverage*

- *Data Accuracy Requirement*
- *Lack of Comprehensive Sources*
- *Insufficient Detail*


01
Fragmented Information Sources
02
Lack of Comprehensive Data
03
Rapid and Dynamic Evolution
04
Extensive Data Parsing Requirements

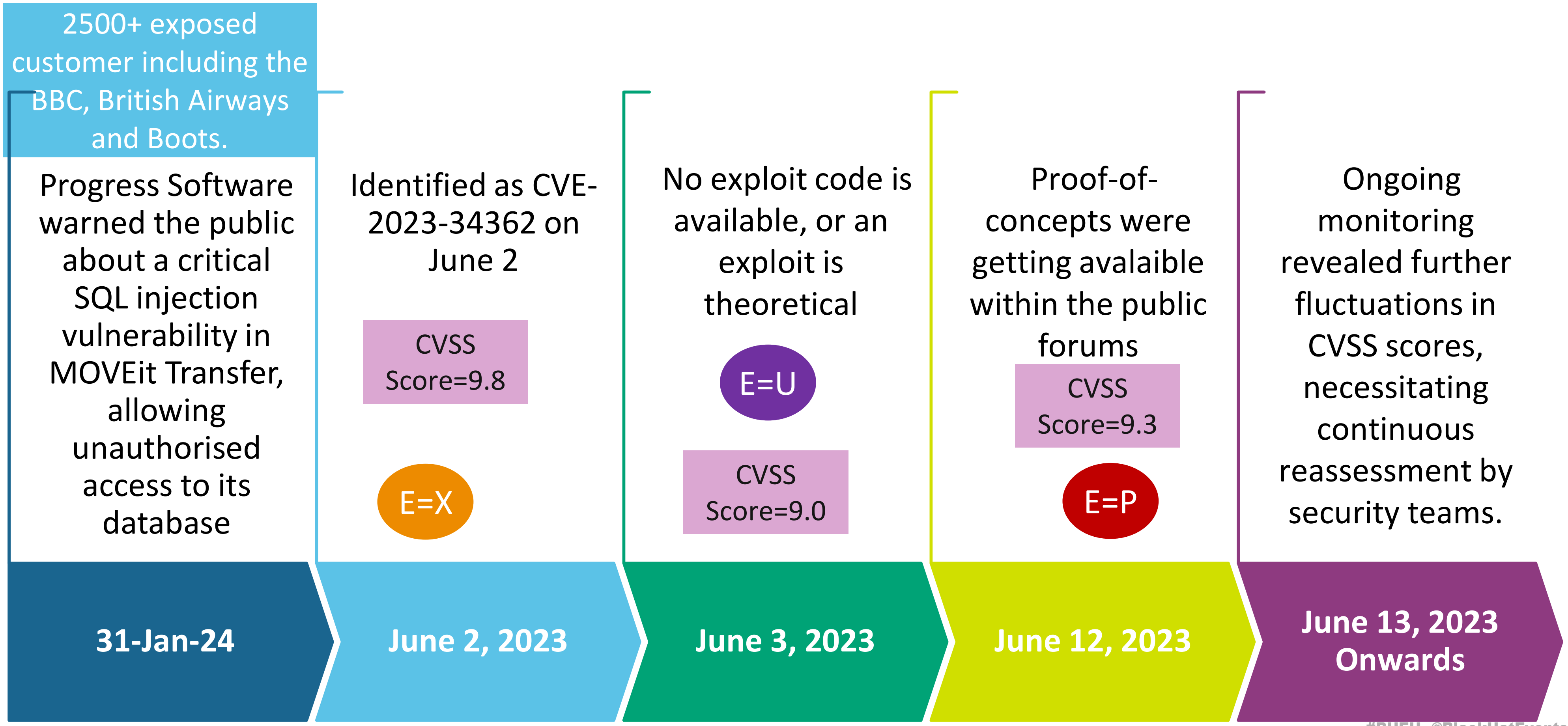
- *Rapid Exploit Development*
- *Data Source Limitations*
- *Outdated Information*

- *Vast Data Volume:*
- *Point-in-Time Accuracy*
- *Continuous Intelligence Challenge*

No official CVSS guidance on appropriate monitoring sources or recommended monitoring frequency.

4 - Exploit Code Maturity Overhead – Case Study

Exploit Maturity Journey for CVE-2023-34362 Progress MOVEit Transfer SQL Injection Vulnerability



2500+ exposed customer including the BBC, British Airways and Boots.

Progress Software warned the public about a critical SQL injection vulnerability in MOVEit Transfer, allowing unauthorised access to its database

31-Jan-24

Identified as CVE-2023-34362 on June 2

CVSS Score=9.8

E=X

June 2, 2023

No exploit code is available, or an exploit is theoretical

E=U

CVSS Score=9.0

June 3, 2023

Proof-of-concepts were getting avalaible within the public forums

CVSS Score=9.3

E=P

June 12, 2023

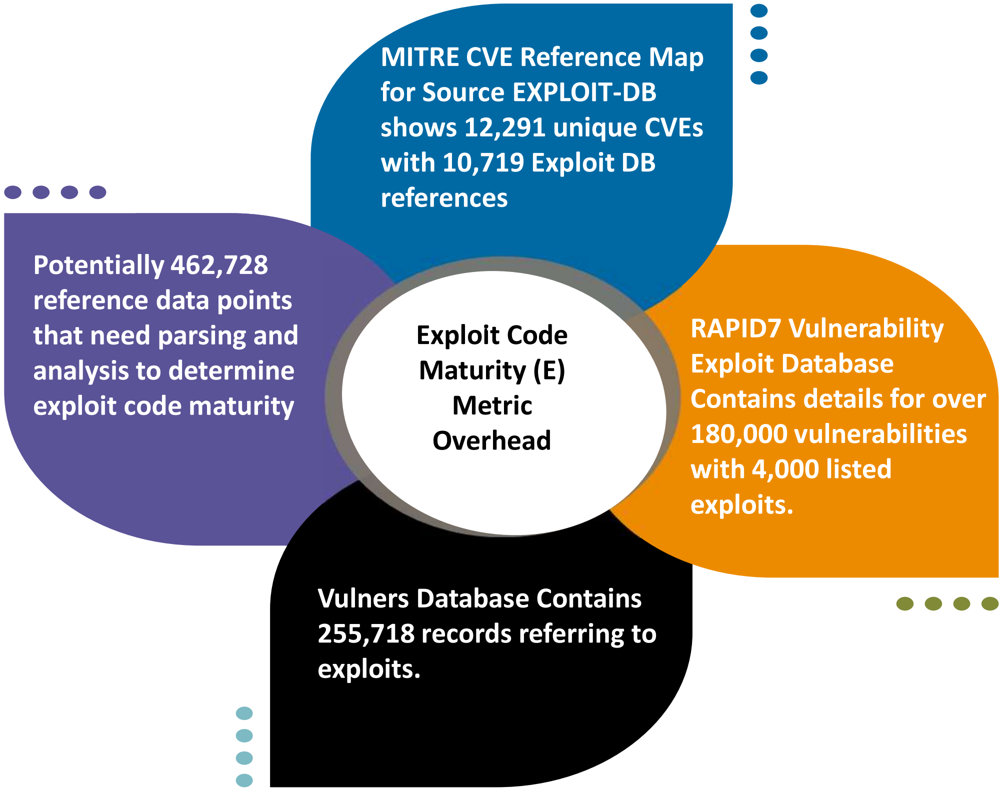
Ongoing monitoring revealed further fluctuations in CVSS scores, necessitating continuous reassessment by security teams.

June 13, 2023 Onwards

Source: https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/ and https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/

4 - Exploit Code Maturity Overhead - Statistics & Impact

Exposure and Impact Radius



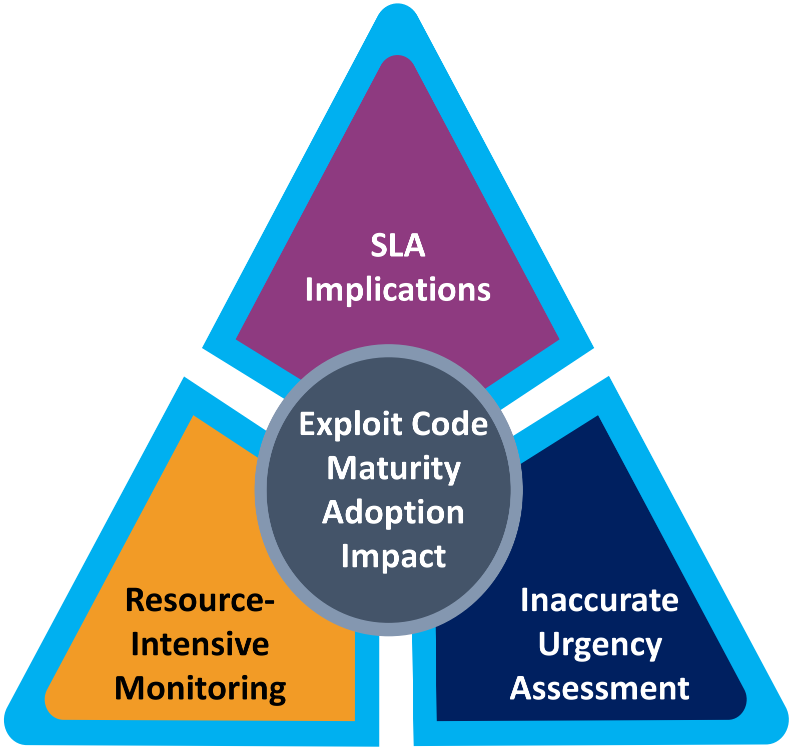
Exploit Code Maturity (E) Metric Overhead

MITRE CVE Reference Map for Source EXPLOIT-DB shows 12,291 unique CVEs with 10,719 Exploit DB references

RAPID7 Vulnerability Exploit Database Contains details for over 180,000 vulnerabilities with 4,000 listed exploits.

Vulners Database Contains 255,718 records referring to exploits.

Potentially 462,728 reference data points that need parsing and analysis to determine exploit code maturity



Exploit Code Maturity Adoption Impact

SLA Implications

Inaccurate Urgency Assessment

Resource-Intensive Monitoring

4 - Exploit Code Maturity Overhead - Recommendation

Recognizing Current Challenges and Providing Strategic Recommendations

Challenge Awareness:

- Lack of an authoritative source for exploit code maturity journey.
- Ever-growing volume of disparate data that requires regular analysis.
- Incorrect or incomplete data could lead to reduced scores and severity ratings.

Recommendation:

- Avoid using the Exploit Code Maturity Metric of the CVSS 3.0/3.1 framework due to the lack of a validated and reliable data source – avoiding artificial lowering of score.

5- Disconnect in APT & Exploitability

Together We Rise: Challenges Demand Unity

5 - Disconnect in APT and Exploitability - Issue Details

Advanced Persistent Threat (APT) and CVSS

Source: https://www.forenova.com/blog/deep-dive-into-advanced-persistent-threats

- **APTs (Advanced Persistent Threats):** sophisticated threats to digital security, often evading traditional security measures.

- **Global Presence**: Over 200 APTs exist globally, including those backed by nation-states and eCriminals.

- **Exploitation of Vulnerabilities**: APTs exploit known vulnerabilities, highlighting the necessity of understanding these threats for effective cybersecurity.

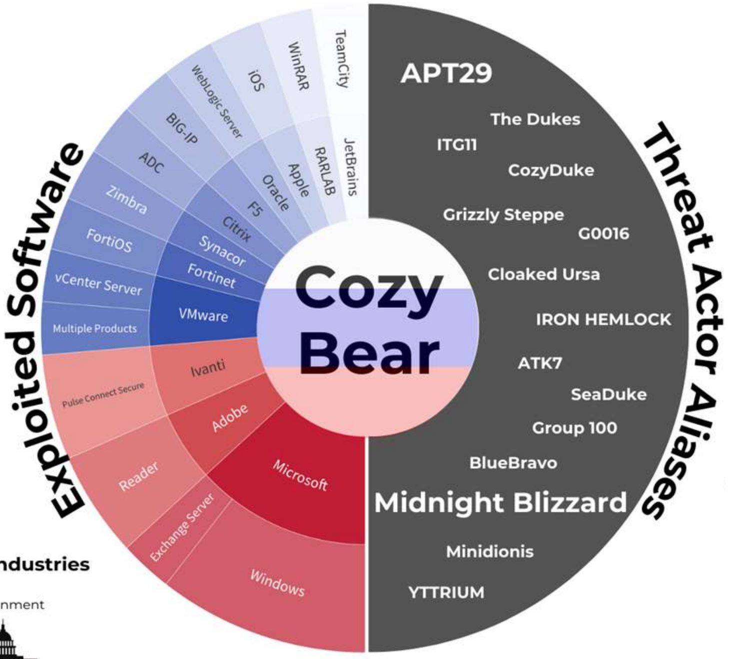
5 - Disconnect in APT and Exploitability - Case Study

Advanced Persistent Threat (APT) and Known CVE Associations

Threat Actor Profile - Cozy Bear (Espionage)

MITRE ATT&CK® Techniques

T1001	T1053-005	T1090-003	T1203	T1547-009	T1566-002
T1027	T1059-006	T1090-004	T1204-002	T1547-001	T1583-006
T1027-002	T1059-001	T1095	T1218-011	T1548-002	T1587-003
T1043	T1070-004	T1102-002	T1546-003	T1550-003	
T1047	T1078-002	T1190	T1546-008	T1566-001	



Known Exploited CVEs

CVE-2010-0232	CVE-2019-9670	CVE-2020-14882	CVE-2021-36934
CVE-2010-4398	CVE-2019-11510	CVE-2021-21972	CVE-2022-30170
CVE-2013-0640	CVE-2019-19781	CVE-2021-26855	CVE-2023-38831
CVE-2013-0641	CVE-2020-4006	CVE-2021-1879	CVE-2023-42793
CVE-2018-13379	CVE-2020-5902	CVE-2021-22893	

Suspected Victim Countries

United States	Begium	Ukraine	Kazakhstan	South Korea
Mexico	Portugal	Romania	China	Japan
Brazil	Georgia	Turkey	India	New Zealand

Target Industries

Government

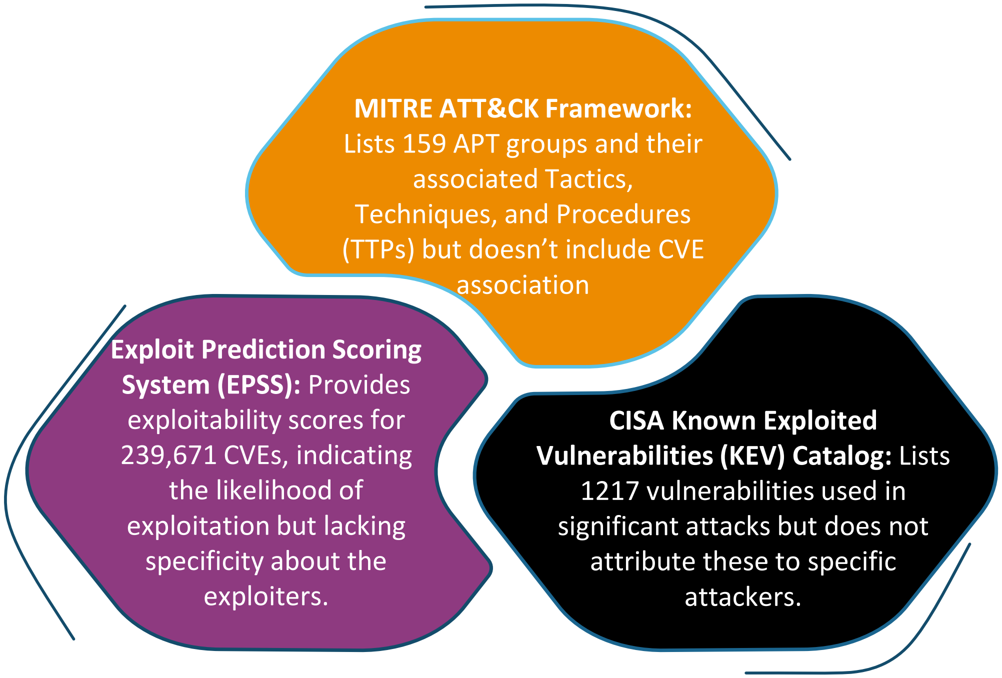
Private Sector

Source: https://vulncheck.com/blog/how-we-think-about-threat-actors

5 - Disconnect in APT and Exploitability- Statistics & Impact

Exposure and Impact Radius

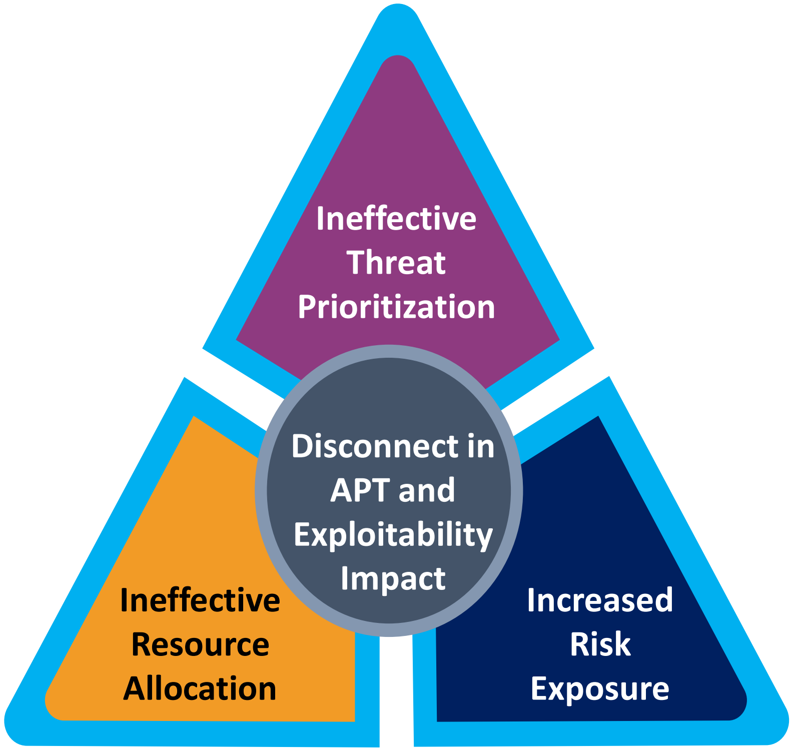
No single source links vulnerabilities to specific threat actors, limiting threat understanding.



MITRE ATT&CK Framework: Lists 159 APT groups and their associated Tactics, Techniques, and Procedures (TTPs) but doesn't include CVE association

Exploit Prediction Scoring System (EPSS): Provides exploitability scores for 239,671 CVEs, indicating the likelihood of exploitation but lacking specificity about the exploiters.

CISA Known Exploited Vulnerabilities (KEV) Catalog: Lists 1217 vulnerabilities used in significant attacks but does not attribute these to specific attackers.



Ineffective Threat Prioritization

Disconnect in APT and Exploitability Impact

Ineffective Resource Allocation

Increased Risk Exposure

5 - Disconnect in APT and Exploitability- Recommendation

Recognizing Current Challenges and Providing Strategic Recommendations

Challenge Acknowledgement:

- APTs often exploit known CVEs, highlighting the need for effective vulnerability management.
- There is no single source of truth for CVE association to APTs within the industry.
- Lack of APT-Specific considerations in CVSS

Recommendation:

- We invite industry to unite in forming solutions for monitoring APT activities and TTPs, **prioritizing vulnerabilities linked to actively exploited CVEs** by incorporation into the CVSS framework.

6- Overlooked Privacy Aspect

Together We Rise: Challenges Demand Unity

6 - Overlooked Privacy Aspect – Issue Details

Security, Privacy and CVSS

Security vs. Privacy

- **Security**: Protects data from unauthorized access and ensures integrity and availability.
- **Privacy**: Protects personal information and controls data sharing with consent.

CVSS and Privacy

- CVSS focuses on exploitability and impacts on confidentiality but neglects privacy implications.
- Privacy is not explicitly included in CVSS scoring.

6 - Overlooked Privacy Aspect- Case Study

Case Study- Real-World Examples showing Privacy risk with underrepresented CVSS Score

Source: https://www.kolide.com/blog/zoom-webcam-hijacking-are-your-users-vulnerable
*https://www.demandsage.com/zoom-statistics/

- ***Use case:*** *Information Disclosure (Webcam) —CVE-2019–13450 vulnerability against zoom clients.*
- ***Zoom has 300 million daily active users as of 2024*.***

- **Exploitation Details**: This vulnerability allows any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission.

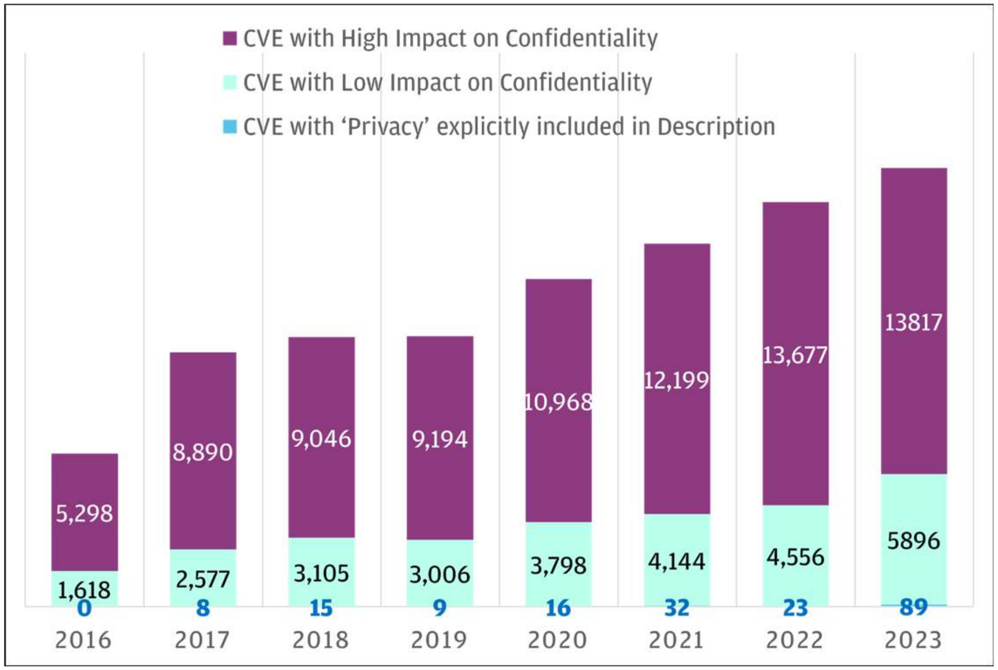
Impact: Cause privacy violations, security risks, potential legal and reputational consequences.

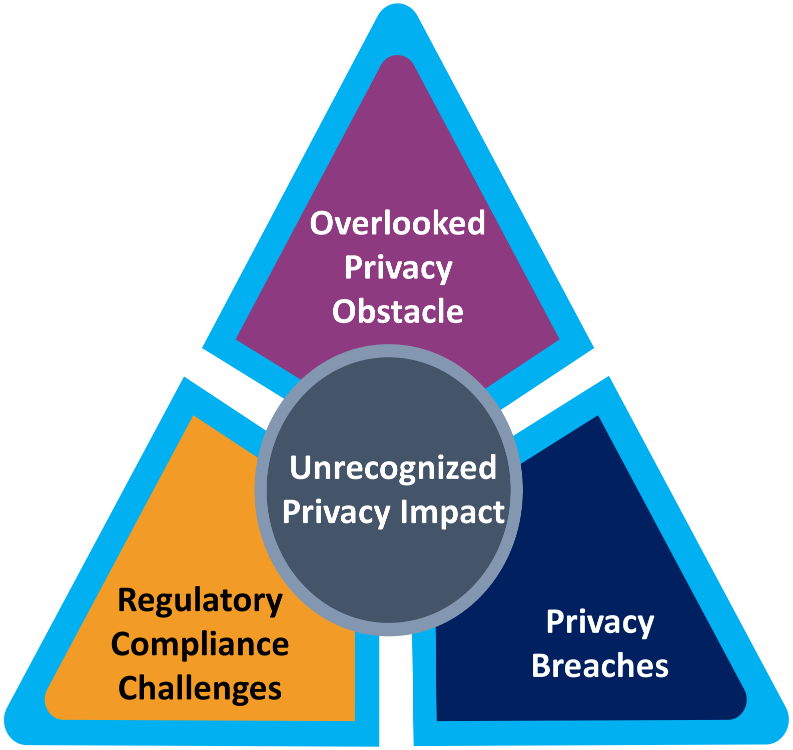
CVSS Rating
Medium

6 - Overlooked Privacy Aspect - Statistics & Impact

Exposure and Impact Radius

CVEs with Confidentiality Impact
vs *Privacy Impact*




Overlooked Privacy Obstacle
Unrecognized Privacy Impact
Regulatory Compliance Challenges
Privacy Breaches

6- Overlooked Privacy Aspect - Recommendation

Recognizing Current Challenges and Providing Strategic Recommendations

Challenge Acknowledgement:

- Blurring of privacy and security boundaries.
- CVSS emphasizes exploitability and confidentiality but overlooks severe privacy implications.
- Nuanced vulnerability assessment needed for privacy-sensitive sectors.

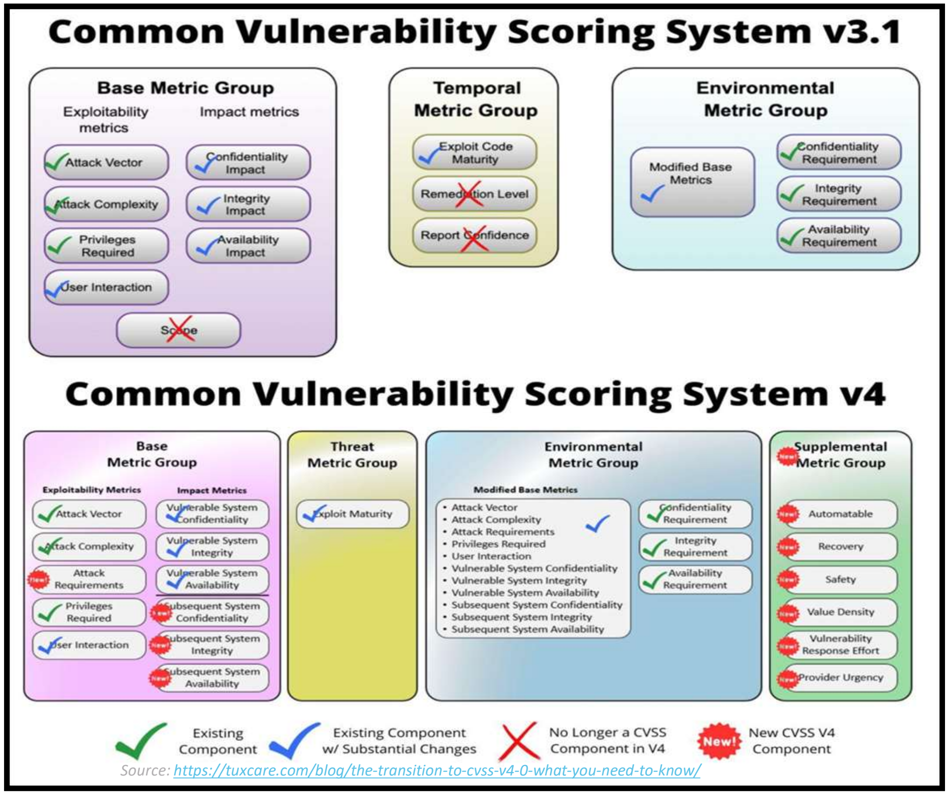
Recommendation:

- Develop **privacy-specific metrics** for assessing vulnerabilities
- Integrate privacy considerations into vulnerability management
- Adopt and leverage privacy frameworks

Moving Past CVSS 3.1

Future Directions : CVSS V4.0 Details

Does CVSS v4 address these Challenges?



Source: https://tuxcare.com/blog/the-transition-to-cvss-v4-0-what-you-need-to-know/

- **Enhancements in Metrics:** CVSS 4.0 introduces expanded impact metrics, refined temporal metrics and new supplemental metrics to improve assessment accuracy.

- **Adoption Trends:** CVSS 4.0 is yet to be fully adopted by security vendors and the NVD, but trends indicate growing interest.

- **Our Initial Review:** Review of the CVSS v4 documentation provided by FIRST, indicates that our operational challenges, such as the lack of privacy considerations and APT associations, persist. Further empirical data and practical implementation guidance will be crucial for necessary validation.

Future Directions : Proposed Extension Metrics

Towards a Solution – what do we need in the framework?

Metric Category	Metric Name	Parameters with desired contribution in overall scoring		
Threat Intelligence	APT Associations [AP]	Yes ⊕	No ●	Not Defined ●
Operating Environmental Context	Environmental Dependency [ED]	Not met ⊖	Met ⊕	Not Defined ●
	Privacy Impact [PI]	Yes ⊕	No ●	Not Defined ●
	Critical Business Services Impact [CB]	Yes ⊕	No ⊖	Not Defined ●

⊕ Increase Score ⊖ Decrease Score ● No Impact

Key Takeaways

Key Takeaways and Q&A

Key Takeaways

1 **Detection Dynamics: Key Patterns**

For Challenges 1 and 2 - Essential Patterns are provided for Monitoring and Strategic Implementation recommended for CVSS v3.0/3.1 users.

2 **Tactical Sparks: Instant Impact**

For Challenges 3 and 4 – Initial ideas for Immediate Impact are provided for Monitoring and Strategic Implementation recommended for CVSS v3.0/3.1 users.

3 **Together We Rise: Challenges Demand Unity**

Challenges 5 and 6 - Substantial and require industry collaboration and effort to resolve, we are actively seeking opportunities for partnership and cooperation.

4 **Towards the Future**

We have outlined additional metrics for consideration, including Threat Intelligence and Operating Environmental Context with Environmental Dependency, Privacy Impact, and Critical Business Services Impact.