KISA KOREA INTERNET & SECURITY AGENCY

Simulation Analysis of Vulnerability Assessment Using CVSS 4.0

Cho Seung Hyun

Korea Security & Internet Agency (KISA, KrCERT/CC)

Who AM I?

Cho Seung Hyun (aka NetKingJ)

O Vulnerability Research Background

- Offensive Security Research

O 10+ Bug Bounty Reports (Samsung Electronics)

- Total Rewards : $20,000+

O Operating Cyber Security RSS Platform

- Domestic and international cybersecurity issue search service
- Link : https://csr.netking.kr

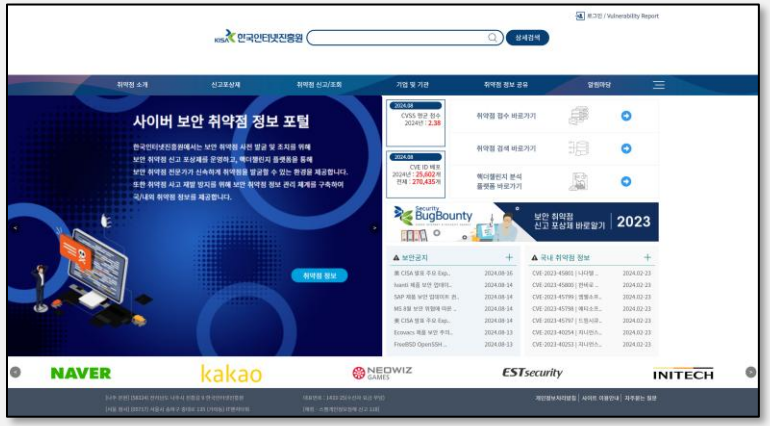
Korea Internet & Security Agency (KISA)

O Affiliation

- Digital Threat Response Division, Vulnerability Analysis Team

O Main Tasks

- Operate a reporting and reward system (Bug Bounty)
- Manage national vulnerability data (KVE, Korea Vulnerability and Exposure)
- Discover vulnerabilities and respond with appropriate measures



https://knvd.krcert.or.kr

Overview of KISA Bug Bounty

History

· A government-led bug bounty program in the Republic of Korea, in operation since 2012

Purpose

· Proactively respond to newly identified security vulnerabilities in software and systems by receiving vulnerability reports

Achievements

· Since its implementation, over 13,678 vulnerabilities have been reported through 2025

Reward System

· Rewards of up to ₩10 million (approx. $7,500 USD) are provided based on CVSS scores and impact factors

Reporting Process (Report → Validation → Decision → Evaluation → Closure)

· Report: The vulnerability is submitted and registered in the system
· Validation: The report is reviewed and the vulnerability is verified
· Decision: A determination is made on whether remediation is necessary
· Evaluation: The reward is assessed based on severity and impact
· Closure: The assessment is finalized and the process is completed

* Vulnerability Reports Over 5 Years (Unit: Count)

	2020	2021	2022	2023	2024
Submissions	1,448	1,727	1,963	1,877	1,786
Valid Reports	589	944	792	957	670
Reward	542	667	671	566	611

* Vulnerabilities by Product Group for the Last 5 Years (Unit: Count)

	2020	2021	2022	2023	2024
Service	838	1,180	1,157	868	1,277
Application	266	212	188	361	193
IoT	141	183	333	443	178

Research Background and Objectives

Step.1

Research Objective

- Analyze changes in vulnerability assessment results after adopting CVSS 4.0
- Evaluate the impact of CVSS 4.0 on the KISA bug bounty system

Step.2

Dataset Composition

- CVE Case Dataset: Public CVEs disclosed in NVD
- KVE Dataset: Domestic vulnerabilities reported via the KISA bug bounty program
- Synthetic Dataset: All possible combinations of CVSS 4.0 metric values

Step.3

Simulation Method

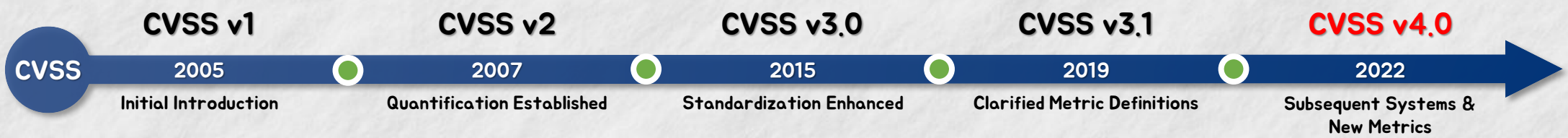
- Perform score calculation using the official CVSS 4.0 calculator and specification by FIRST

Step.4

Analysis Details

- Aggregate cases with score increases, decreases, or no changes between CVSS 3.1 and 4.0
- Conduct sensitivity analysis to evaluate the influence of each metric on the final score

Overview of CVSS



○ CVSS (Common Vulnerability Scoring System)

① Quantitative Assessment

- Evaluates vulnerability severity numerically from 0.0 to 10.0
- Valid vulnerabilities have scores above 0.1

② Standardized Measurement

- Provides a consistent method to understand and share vulnerability severity
  - › e.g., CVSS:4.0/AV:A/AC:H/AT:P/PR:H/UI:P/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

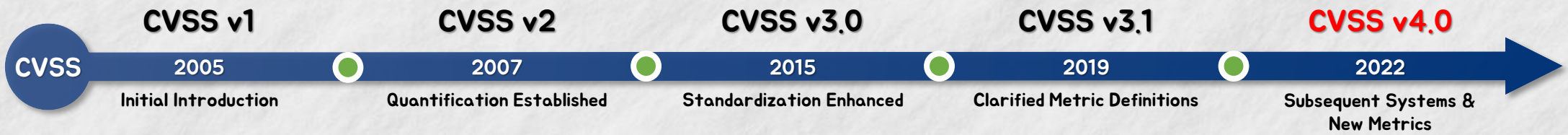
③ Risk Classification

- Requires rapid response for high-scoring vulnerabilities
  - › Categories: None(0.0), Low(0.1~3.9), Medium(4.0~6.9), High(7.0~8.9), Critical(9.0~10.0)

④ Evaluation Factors

- Exploitability Metrics
  - › Attack Vector (AV), Attack Complexity (AC), Attack Requirements (AT), Privileges Required (PR), User Interaction (UI)
- Vulnerable System Impact Metrics
  - › Confidentiality (VC), Integrity (VI), Availability (VA)
- Subsequent System Impact Metrics
  - › Confidentiality (SC), Integrity (SI), Availability (SA)

Overview of CVSS



○ Limitations of the Existing CVSS 3.1 Framework

① Insufficient Evaluation Items

· Does not fully reflect evolving attack techniques and complex vulnerability scenarios
  › e.g., Conditions needed for an attack, system-wide impact via chained vulnerabilities

② Score Distribution Imbalance

· Many vulnerabilities cluster within certain score ranges, making it difficult to reflect actual risk

③ Scope (S) Limitations

· Limited coverage of impacts on subsequent systems* hinders overall risk assessment

· Example of Subsequent Systems: Host impacts from vulnerabilities in virtualization (e.g., VMware)

Key Changes in CVSS 4.0 : Added and Modified Vulnerability Evaluation Metrics

① Attack Requirements (AT) → Newly Added

· Evaluation Method: Existence of requirements necessary for an attack

· Metrics
› None (N) : Attack can be executed without prerequisites
›› e.g., SQL Injection on a website
› Present (P) : Specific conditions required to execute an attack
›› e.g., attack possible only on software with specific versions or configurations

② User Interaction (UI) → Improved

· Evaluation Method: User involvement necessary for the attack

· Metrics
› None (N) : Attack possible without any user interaction
›› e.g., automated attacks
› Passive (P) : Limited user interaction required
›› e.g., user clicks malicious link
› Active (A) : User performs normal actions unaware of the attack
›› e.g., opening a seemingly legitimate file

③ Scope (S) → Replaced by Impact Metrics

· Removed the traditional scope evaluation and introduced
› Vulnerable System Impact Metrics (VC, VI, VA)
› Subsequent System Impact Metrics (SC, SI, SA)

· Evaluation Metrics

1. Confidentiality (VC/SC)
› None (N) : No loss
› Low (L) : Partial loss, limited privileges gained without full control
› High (H) : Complete loss, full disclosure of all information within the system

2. Integrity (VI/SI)
› None (N) : No loss
› Low (L) : Limited modification of data without direct severe impact
› High (H) : Complete loss, all protected files can be modified

3. Availability (VA/SA)
› None (N) : No impact
› Low (L) : Performance degradation and resource availability interruption
› High (H) : Complete loss of availability, complete denial of resource access

· Ex) S = Changed (C)
› A vulnerability in a virtual machine allowing access to host OS files impacts both the virtual machine (vulnerable system) and the host OS (subsequent system)

· Ex) S = Unchanged (U)
› Opening a malicious PDF affects only the document itself without influencing other files or systems, resulting in no subsequent system impact

Comparison Between CVSS 3.1 and CVSS 4.0 : Grouping and Mapping

O Introduction of EQ Elements

· Detailed scoring through the application of formulas (EQ1~EQ6) for metric groups

· **Exploitability**
  › Attack Vector (AV), Privilege Required (PR), User Interaction (UI)
  › Scores: High (0), Medium (1), Low (2)
· **Attack Complexity**
  › Attack Complexity (AC), Attack Requirements (AT)
  › Scores: High (0), Medium (1)
· **Vulnerable System Impact**
  › Confidentiality Impact (VC), Integrity Impact (VI), Availability Impact (VA)
  › Scores: High (0), Medium (1), Low (2)
· **Subsequent System Impact**
  › Confidentiality Impact (SC), Integrity Impact (SI), Availability Impact (SA)
  › Scores: High (0), Medium (1), Low (2)
· **Exploitation**
  › Exploit Code Maturity (E)
  › Scores: High (0), Medium (1), Low (2)
· **Security Requirements**
  › Confidentiality Requirement (CR), Integrity Requirement (IR), Availability Requirement (AR)
  › Scores: High (0), Medium (1)

· Each group's score is calculated based on metrics, determining the overall severity of vulnerabilities

* Metric = Vulnerability Evaluation Metrics

O Special Features

· Metric groups' scores are combined into a standardized 6-digit number for easier comparison

· **Score Range**
  › Attack Complexity and Security Requirements: Scores classified as 0 or 1
  › Other groups: Scores classified as 0, 1, or 2

· **Macro Vector**
  › Combination of scores from each group represented as a 6-digit Macro Vector
  › Example: "000000" indicates all groups have a score of 0
  › Macro Vector simplifies the representation of overall vulnerability severity

· **Scoring Table**
  › Predefined CVSS scores corresponding to each Macro Vector
  › Example: "000000" = 10, "000001" = 9.9 , etc.

· **Distribution Chart**
  › Analysis of CVSS score distribution based on possible Macro Vector combinations
  › Example Distribution: 0.1: 212221, 0.2: 211221, etc.

· **Missing Scores**
  › Certain score ranges do not exist in Macro Vector combinations
  › For example, no combination results in scores in the 3-point range from basic metric combinations.

Comparison Between CVSS 3.1 and CVSS 4.0 : Relative Impact Analysis

CVSS 3.1

① Confidentiality (C) : 2.2994212962962965
② Integrity (I) : 2.2994212962962965
③ Availability (A) : 2.2994212962962965
④ Attack Vector (AV) : 1.497067901234568
⑤ Scope (S) : 1.0171296296296297
⑥ Privileges Required (PR) : 0.9280092592592593
⑦ Attack Complexity (AC) : 0.6986111111111111
⑧ User Interaction (UI) : 0.40092592592592596

* Analysis Method : After extracting all evaluation items from CVSS 4.0, the relative influence was calculated based on the rate of score changes for each item

CVSS 4.0

① Attack Vector (AV) : 1.8939605243103186 => 3↑
② Confidentiality (VC) : 1.7649405578417925 => 1↓
③ Integrity (VI) : 1.7649405578417925 => 1↓
④ Availability (VA) : 1.3560785322359397 => 1↓
⑤ Privileges Required (PR) : 0.7732167352537723 => 1↑
⑥ User Interaction (UI) : 0.7732167352537723 => 2↓
⑦ Confidentiality (SC) : 0.7620056012802927 => New
⑧ Integrity (SI) : 0.7620056012802927 => New
⑨ Availability (SA) : 0.7620056012802927 => New
⑩ Attack Complexity (AC) : 0.6642184880353604 => 3↓
⑪ Attack Requirements (AT) : 0.6642184880353604 => New

Comparison Between CVSS 3.1 and CVSS 4.0 : Score Distribution and Changes

O Methodology

· CVSS 4.0 to 3.1 Vector Conversion Rules

› User Interaction (UI)
  >> N → N (CVSS 3.1)
  >> R or A → R (CVSS 3.1)

› Scope (S) Determination
  >> If all of SC, SI, SA = N → S:U (Unchanged)
  >> If any of SC, SI, SA ≠ N → S:C (Changed)

· Exhaustive Evaluation of All CVSS 4.0 Combinations

› Python was used to generate all possible metric combinations of CVSS 4.0 and compute the corresponding base scores

O Summary of Findings

· Number of Combinations

› Base Metrics only: 104,976

› All Metrics (Expanded): 906,992,609

· Score Difference Range

› From -5.1 to +7.9

· Count of Score Changes

› Increased: 42,962 cases

› Decreased: 58,576 cases

› Unchanged: 3,438 cases

· Key Observations

› No score exists in the 3-point range under CVSS 4.0 Base Metrics

› CVSS 3.1 shows a relatively Gaussian distribution, while CVSS 4.0 does not exhibit such a shape

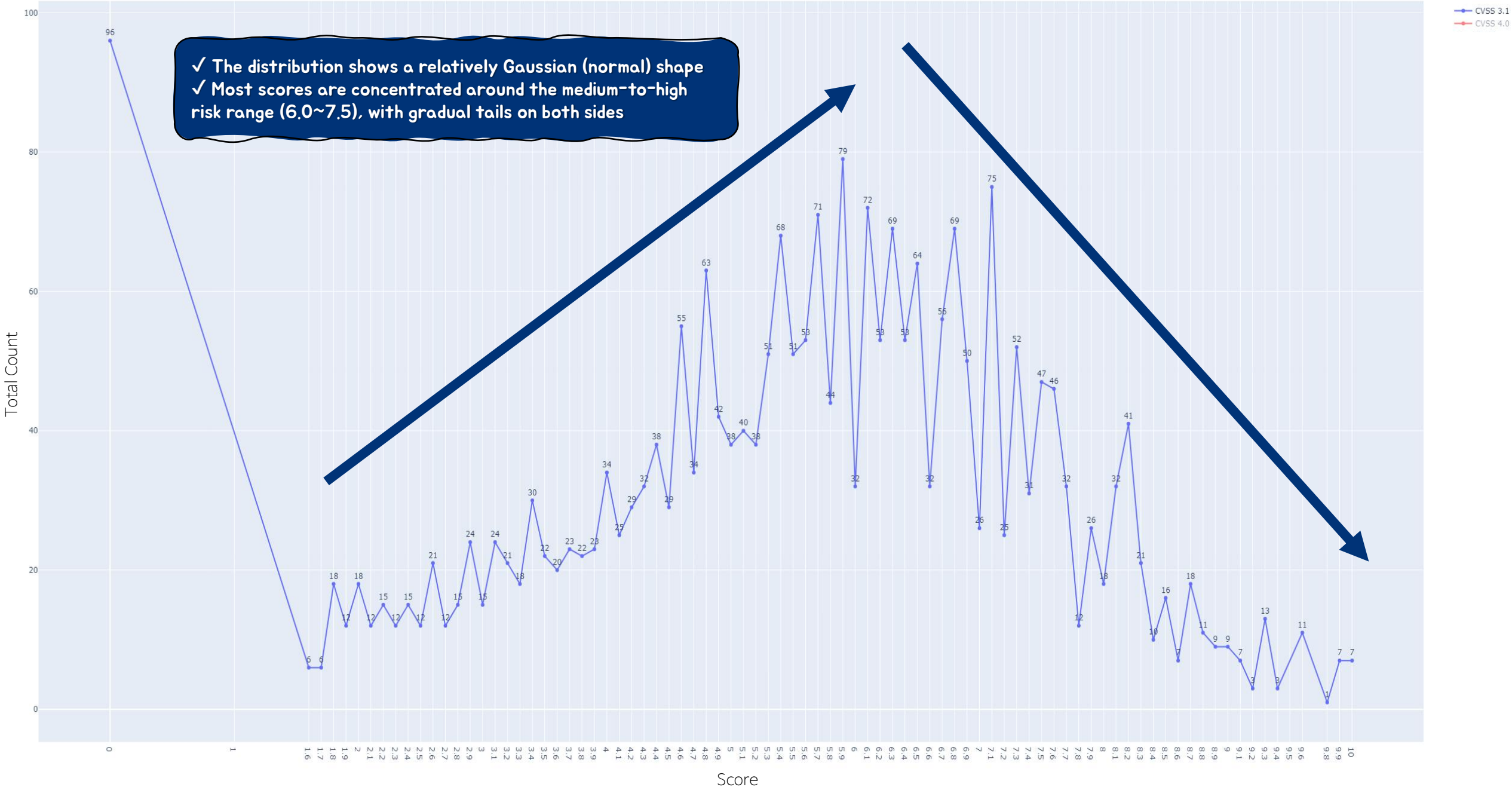
Comparison Between CVSS 3.1 and CVSS 4.0 : Score Distribution and Changes

○ Python Code for Generating All CVSS 4.0 Base Metric Vectors

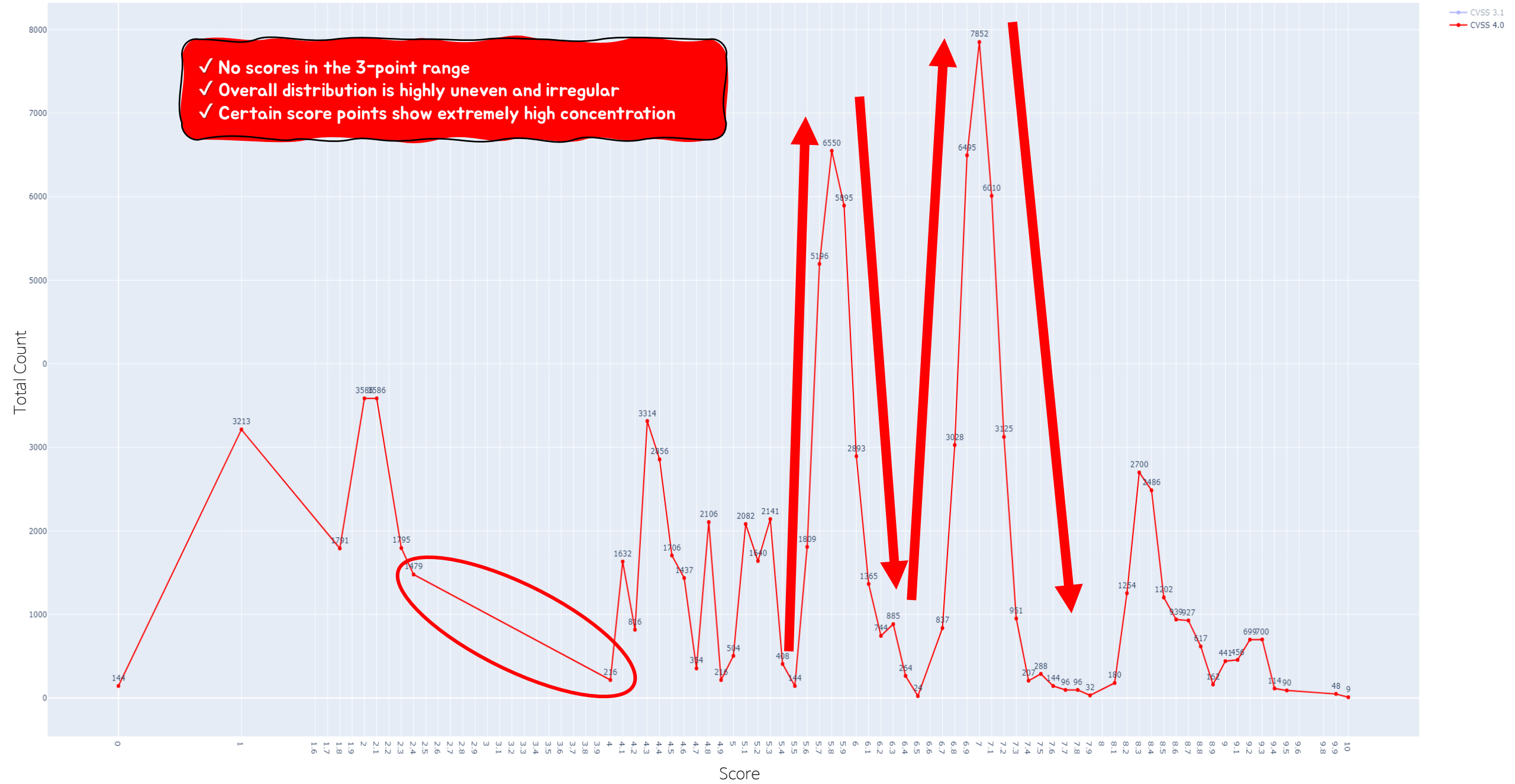
```
from itertools import product
from cvss import CVSS4
metrics = {
    'AV': ['N', 'A', 'L', 'P'],
    'AC': ['L', 'H'],
    'AT': ['N', 'P'],
    'PR': ['N', 'L', 'H'],
    'UI': ['N', 'P', 'A'],
    'VC': ['H', 'L', 'N'],
    'VI': ['H', 'L', 'N'],
    'VA': ['H', 'L', 'N'],
    'SC': ['H', 'L', 'N'],
    'SI': ['H', 'L', 'N'],
    'SA': ['H', 'L', 'N']
}
metric_keys = list(metrics.keys())
all_combinations = product(*(metrics[m] for m in metric_keys))

with open('cvss4.0_combinations.txt', 'w') as f:
    for combo in all_combinations:
        vector = 'CVSS:4.0/' + '/'.join(f"{k}:{v}" for k, v in zip(metric_keys, combo))
        score = CVSS4(vector).scores()[0]
        f.write(f"{vector}\t{score}\n")
```

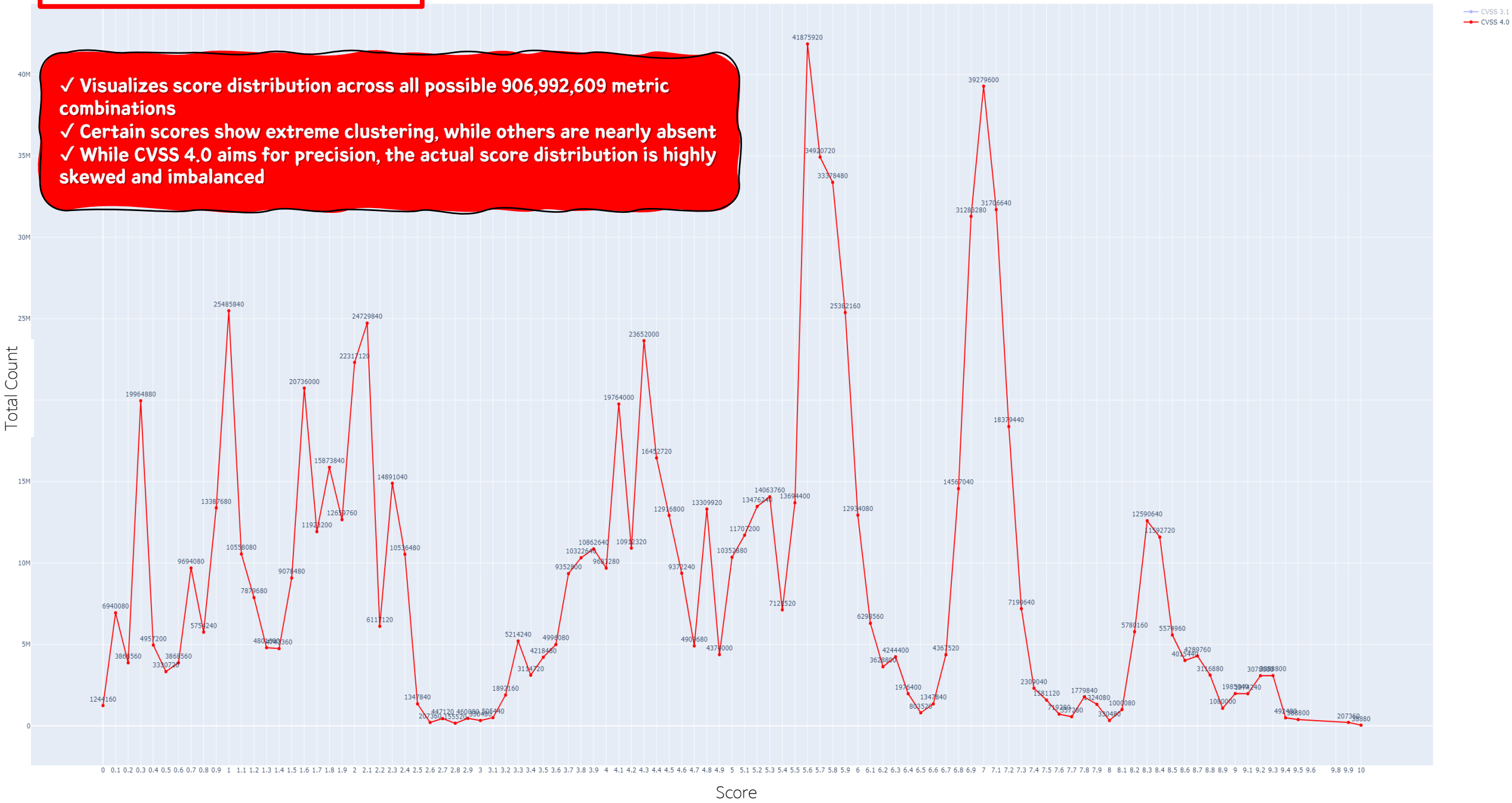
CVSS 3.1 Score Distribution



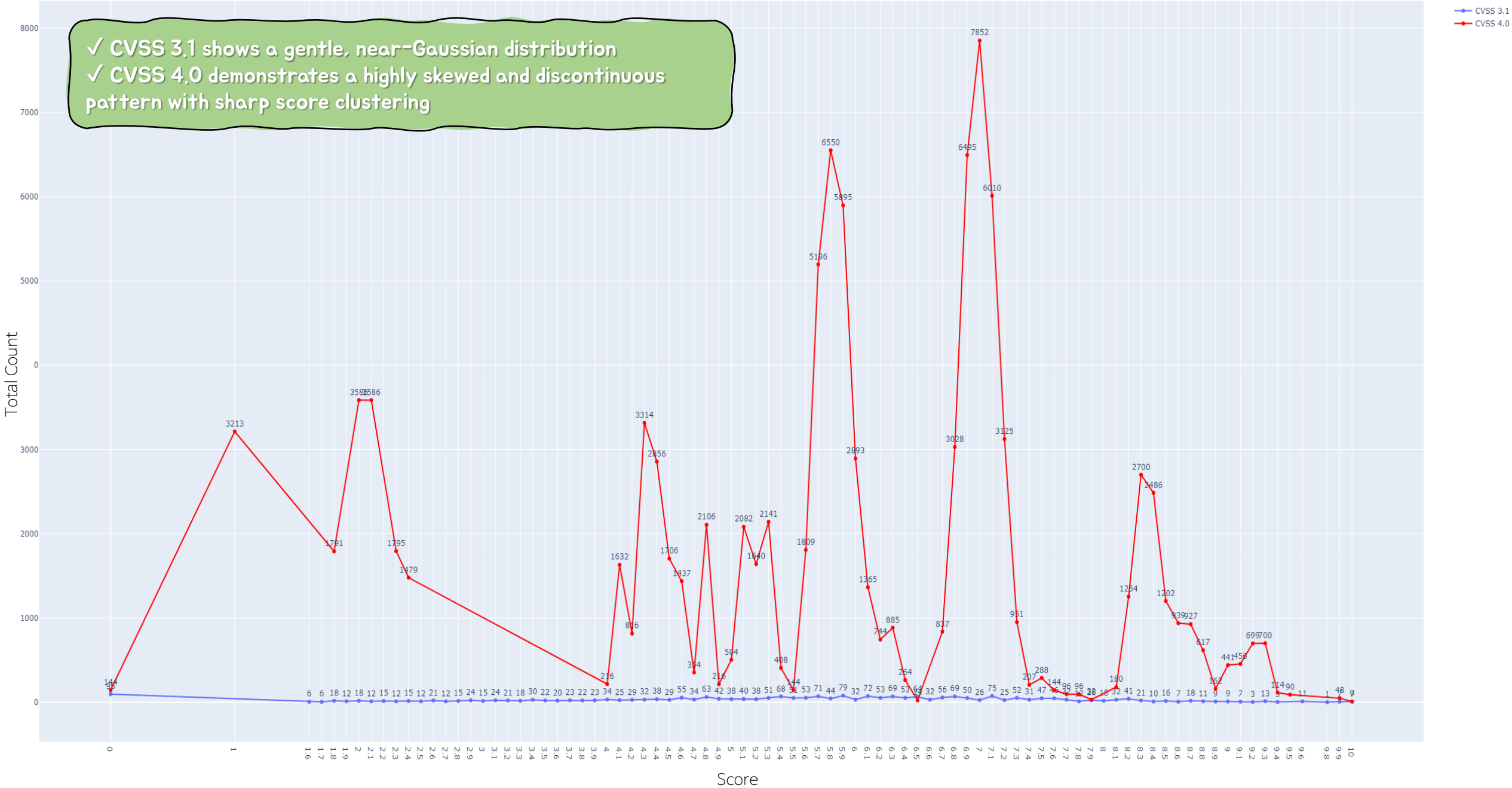
CVSS 4.0 Score Distribution



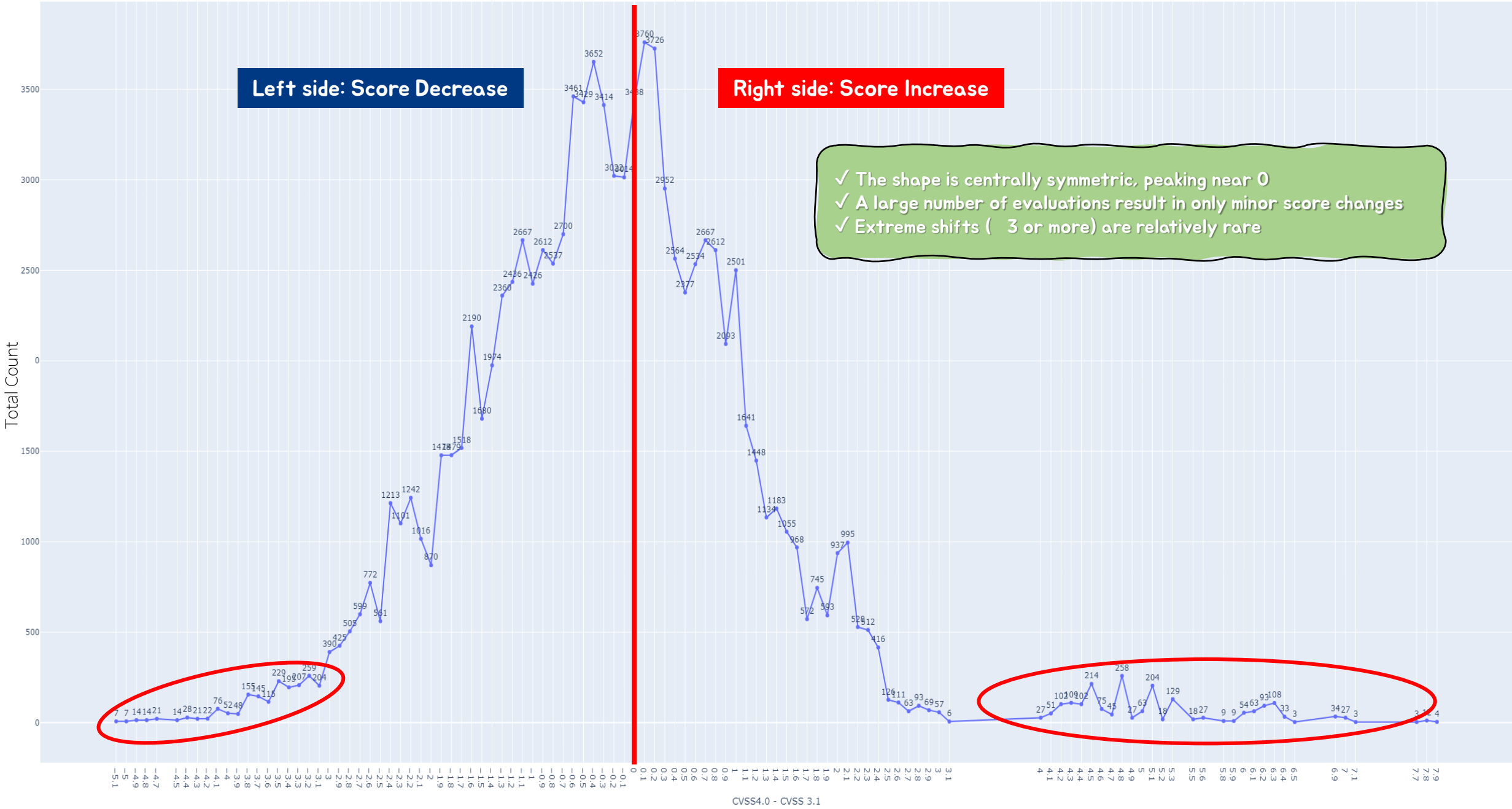
CVSS 4.0 Score Distribution



CVSS 3.1 vs CVSS 4.0 Score Distribution Comparison



CVSS 3.1 / CVSS 4.0 Score Difference Distribution



Comparison Between CVSS 3.1 and CVSS 4.0 : Score Distribution Analysis

○ Notable Points in Score Comparison

· (Underrated Cases) Cases where the CVSS 3.1 score is 0, but a score is assigned in CVSS 4.0 (Total: 124 cases)

CVE	AV	AC	AT (4.0)	PR	UI (3.1)	UI (4.0)	VC	VI	VA	S (3.1)	SC (4.0)	SI (4.0)	SA (4.0)	3.1 Score	4.0 Score	DIFF
CVE-2024-21544	N	L	N	N	N	N	N	N	N	C	H	N	N	0	7.7	+7.7
CVE-2024-10125	N	L	P	N	N	N	N	N	N	C	H	L	N	0	6.9	+6.9
CVE-2025-24320	N	L	N	L	R	P	N	N	N	C	L	L	N	0	5.1	+5.1
CVE-2024-45385	N	H	N	N	R	A	N	N	N	C	L	L	N	0	2.1	+2.1

› In CVSS 3.1, if confidentiality (C), integrity (I), and availability (A) are all 'None (N)', the score is 0. However, if the scope (S) is 'Changed (C)', follow-up system impact is considered

› In CVSS 4.0, follow-up system metrics (SC, SI, SA) are introduced, and a score is assigned if any of them are not 'None (N)'

Comparison Between CVSS 3.1 and CVSS 4.0 : Score Distribution Analysis

○ Notable Points in Score Comparison

· (Overrated Cases) Cases where CVSS 3.1 score is 10, but CVSS 4.0 score is less than 10 (Total: 12 cases)

CVE	AV	AC	AT (4.0)	PR	UI (3.1)	UI (4.0)	VC	VI	VA	S (3.1)	SC (4.0)	SI (4.0)	SA (4.0)	3.1 Score	4.0 Score	DIFF
CVE-2024-11317	N	L	N	N	N	N	H	H	L	C	L	L	L	10.0	9.3	-0.7
CVE-2024-51555	N	L	N	N	N	N	H	H	H	C	L	L	L	10.0	9.3	-0.7
CVE-2024-52329	N	L	P	N	N	N	H	H	N	U	H	H	H	10.0	9.5	-0.5
CVE-2024-56336	N	L	P	N	N	N	H	H	H	U	H	H	H	10.0	9.5	-0.5

› In CVSS 3.1, a score of 10 is assigned when confidentiality (C), integrity (I), and availability (A) are all rated 'High (H)'

› In CVSS 4.0, the final score may be adjusted based on downstream system impact, so the score may be less than 10 depending on the follow-up system metrics (SC, SI, SA)

Analysis of CVEs Evaluated with CVSS 4.0

O Overview

- A total of 5,388 CVEs were analyzed (as of 2025.03.30)
- Based on CVSS 4.0 : increased 2,613 / decreased 2,659 / unchanged 116
- Some vulnerabilities scored 0 in CVSS 3.1 but received a score in CVSS 4.0

O Notable Observations

- Vulnerabilities that scored 3–5 in CVSS 3.1 often received higher scores in CVSS 4.0
- This is due to CVSS 4.0's more granular evaluation method, which better reflects the actual risk

* Methodology : Only CVEs with available CVSS 4.0 scores were used for statistical analysis
* Reference: https://github.com/CVEProject/cvelistV5

Total	Same	Decreased	Increased	3.1 X	
5,388	116	2,659	2,613	1,543	
4.0	Value	3.1	Value		
0 =	0	0 =	124		
10 =	67	10 =	109		
0 ~ 1	0	0 ~ 1	124		
1 ~ 2	27	1 ~ 2	1		
2 ~ 3	166	2 ~ 3	183		
3 ~ 4	0	3 ~ 4	243		
4 ~ 5	201	4 ~ 5	774		
5 ~ 6	2,152	5 ~ 6	572		
6 ~ 7	1,074	6 ~ 7	1,414		
7 ~ 8	416	7 ~ 8	1,102		
8 ~ 9	897	8 ~ 9	521		
9 ~ 10	375	9 ~ 10	345		
4.0	NONE	LOW	MEDIUM	HIGH	CRITICAL
2016	0	0	1	0	0
2017	0	0	2	3	1
2018	0	0	3	0	1
2019	0	0	0	2	0
2020	0	1	3	13	3
2021	2	1	5	5	0
2022	0	1	7	9	0
2023	0	5	45	66	11
2024	0	113	2.384	983	300
3.1	NONE	LOW	MEDIUM	HIGH	CRITICAL
2016	0	0	1	0	0
2017	0	0	4	1	1
2018	0	0	3	0	1
2019	0	0	0	2	0
2020	0	2	2	15	1
2021	0	0	6	5	0
2022	0	2	8	6	1
2023	1	10	55	51	10
2024	84	220	1.975	1.189	312

KVE Case Analysis Based on CVSS 4.0 Evaluation

Overview

- A total of 285 KVEs analyzed (as of Q4 2024)
- Based on CVSS 4.0, increased 237 / decreased 63 / unchanged 15

- Total reward amount
  - > Based on CVSS 3.1: $111,133
  - > Based on CVSS 4.0: $166,667
  - > + Difference: $55,534 increase (+49.96%)

Key Observations

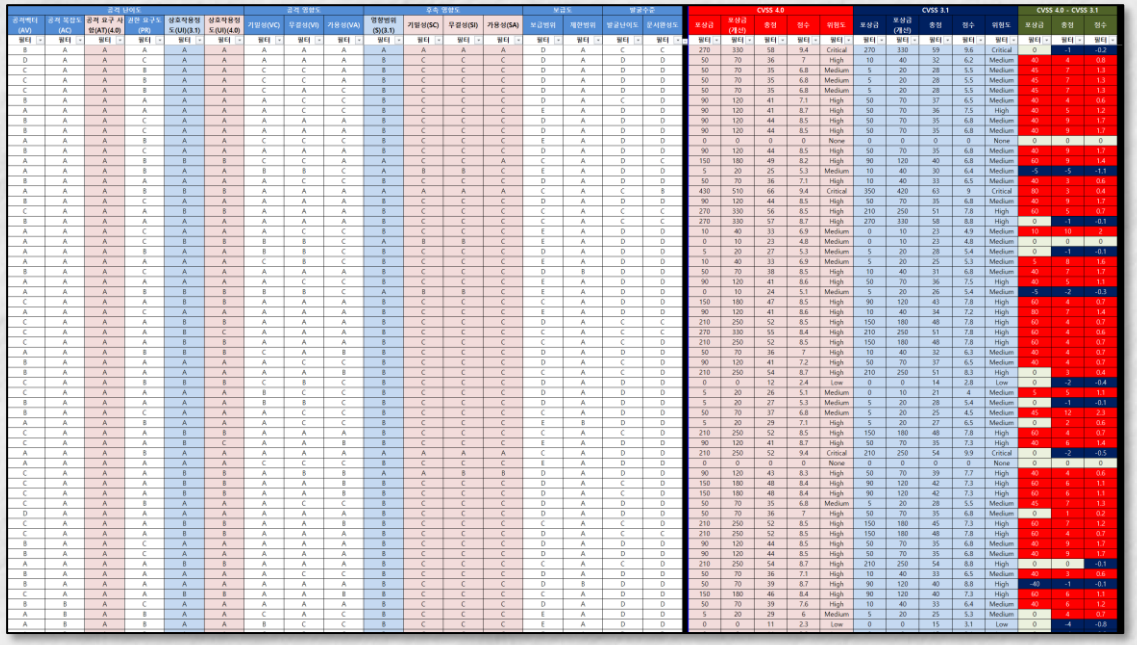
- The introduction of downstream system metrics significantly impacted scores, leading to higher reward payouts

- To ensure fairness and proper budget management, the reward system criteria and payment method may need to be revised

* Evaluation metrics were calculated by applying both CVSS 3.1 and 4.0 to quarterly KVE reports

Quarter	CVSS 3.1 Reward	CVSS 4.0 Reward	Difference	Increase (%)
Q1 2024	$20,333	$28,533	+$8,200	+40.33%
Q2 2024	$29,267	$41,200	+$11,933	+40.77%
Q3 2024	$22,200	$39,600	+$17,400	+78.38%
Q4 2024	$39,333	$57,333	+$18,000	+45.76%
Total	$111,133	$166,667	+$55,534	+49.96%

* Comparison data between CVSS 3.1 and CVSS 4.0 based on vulnerability reports submitted to KISA in 2024



Necessity of Adopting CVSS 4.0

O Reflecting the Evolving Threat Landscape

· New evaluation elements such as impact on downstream systems allow for more accurate assessment of vulnerabilities in complex security environments.
  * e.g., Attack Requirements (AT), User Interaction (UI), Downstream System Impact

O Global Standards and Trends

· The National Vulnerability Database (NVD) has begun partial adoption of CVSS 4.0

· CVSS 3.1 lacks the granularity to reflect new and emerging threats

· Examples of CVEs Evaluated with CVSS 4.0 (Total: 5,388 cases)
  › e.g., CVE-2024-0569, CVE-2024-0570, CVE-2024-1228, CVE-2023-2567, CVE-2024-3699, etc.
  * Some government agencies in South Korea have not yet adopted CVSS 4.0 evaluations

O Improved Assessment Accuracy

· Granular metrics provide a more accurate representation of actual risk
· This supports more effective security response, identifying risks that were previously rated 0 in CVSS 3.1 but scoreable in CVSS 4.0
  * Primarily due to the inclusion of Subsequent System Impact Metrics in the evaluation

Considerations and Implementation Plans for CVSS 4.0 Adoption

O Strengthening Internal Training

· Systematic training is necessary to understand CVSS 4.0's new metrics and evaluation methods

· Implement training programs (e.g., CoP, mock reports/comprehensive evaluations) to enhance evaluator capabilities

· Case of Inadequate Evaluation

› Under CVSS 3.1, if the Scope (S) was rated as "Unchanged (U)," it should consistently be "None (N)" under CVSS 4.0
› In reality, some CNA agencies have made errors when transitioning these ratings

O Revising Evaluation Procedures

· Reexamine reward policies and criteria to align with the new CVSS 4.0 scoring system

· Restructure scoring policies and update related systems

O Changes in Budget Management

· Adjust overall budgets and reward criteria to account for increased payout amounts

· Example from a Bug bounty simulation (Q1–Q4 of 2024)

› CVSS 4.0-based reward: $111,133
› CVSS 3.1-based reward: $166,667
› Increase: Approximately $55,534(+49.96%) more

Considerations and Implementation Plans for CVSS 4.0 Adoption

O Evaluation System Updates

· Improve the vulnerability management system to accommodate CVSS 4.0 scores after analysis

· Phased Adoption Plan

› Test Phase (2024): Pilot CVSS 4.0 for bug bounty program vulnerabilities
› Full Implementation (Q1 2025): Apply CVSS 4.0 to all bug bounty programs and security advisories
› Monitoring and Feedback: Identify and resolve issues arising post-adoption

O External Communication

· Actively inform reporters about changes under CVSS 4.0 to minimize confusion.

· Use KISA's Vulnerability Portal and BohoNara* as channels for sharing information and addressing inquiries.
* BohoNara Site : https://boho.krcert.or.kr

O CVSS 4.0 Enhancement Research

· Improving Score Balance: Research optimal metric weighting and calculation formulas.

· Simplifying Calculation Methods: Provide user-friendly calculation tools and guides.

· Clarifying Metric Definitions: Offer consistent evaluation standards and examples to ensure uniform scoring.

KISA KOREA INTERNET & SECURITY AGENCY

Thank you

Cho Seung Hyun

Korea Security & Internet Agency (KISA, KrCERT/CC)

Email : netkingj@kisa.or.kr