2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing

Trend Analysis of the CVE for Software Vulnerability Management

Yung-Yu Chang, Pavol Zavarsky, Ron Ruhl, Dale Lindskog
Information Systems Security Management
Concordia University College of Alberta
Edmonton, Canada
yychang@csa.concordia.ab.ca, {ron.ruhl, pavol.zavarsky, dale.lindskog}@concordia.ab.ca

***Abstract*—Understanding vulnerability trends is a key component of the risk management process. The focus of this research is to analyze the trends of Common Vulnerabilities and Exposures (CVE) from the National Vulnerability Database (NVD) from 2007 to 2010. We extracted 22,521 CVEs through the four years, also collected their Common Vulnerability Scoring System (CVSS) scores from the NVD; then we analyzed the overall frequency, severity, and CVSS base metrics trends. Our finding shows that the frequency of all vulnerabilities decreased by 28% from 2007 to 2010; also, the percentage of high severity incidents decreased for that period. Over 80% of the total vulnerabilities were exploitable by network access without authentication. We further studied the trends of the select fifteen (15) vulnerability types which contain 18,427 vulnerabilities by analyzing their changes in frequency, severity, and CVSS base metrics. This research findings can help information security professionals focus their efforts in preventing and mitigating the impact of the attacks, and influence the development of security strategies developed by IS professionals as well.**

Keywords-vulnerability type; vulnerability trend; CVE; NVD; CVSS version2

I. Introduction

G. Stonebumer et al., described vulnerability as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy [1]. Assessing the potential vulnerability is an important part of risk management. Knowledge of current security vulnerability trends can have significant benefits to a wide range of IT and security professionals in order for them to better prepare in preventing and mitigating the impact of the attacks.

S. Christey et al., in their paper titled "Vulnerability Type Distributions in CVE" studied CVE trends in 2007 analyzing over forty (40) vulnerability types [2]. From their analyzed vulnerabilities, we have selected 15 vulnerability types, which contain 80% of all of the vulnerabilities, based on their high frequency of occurrence. The types that have been selected include: (1) authentication problem, (2) buffer overflow, (3) cryptographic error, (4) Cross-Site Request Forgery (CSRF), (5) Carriage Return Line Feeds (CRLF) injection, (6) directory traversal, (7) Denial of Service (DoS), (8) format-string, (9) information leak/ disclosure, (10) integer overflow, (11) PHP remote file inclusion, (12) privilege action, (13) race condition, (14) SQL injection, (15) Cross-Site Scripting (XSS).

The focus of this research is to analyze the trends of the select vulnerability types using their frequencies and scores from 2007 to 2010. To better understand the distribution of the vulnerability types, we also observed the CVSS base metrics trends of each type. It is expected that this research will focus attention on the vulnerability trends and serve as a reference to various IT and security professionals in software development, antivirus solutions and the establishment of IT security strategies. This paper is presented as follows. Section II discusses the related work. Section III presents the methodology that guides this research. Section IV gives analyzed vulnerability trends while focusing on the select 15 vulnerability types. In section V, we give the conclusion and future work.

II. Related Work

This research referenced the paper "Vulnerability Type Distributions in CVE" [2] by Christey et al. The differences between ours and theirs are the following:

1) Their data collection was from 2001 to 2006, we studied the following years from 2007 to 2010.

2) They listed roughly 40 vulnerability types and studied their trends. We selected the 15 vulnerability types based on their flaw definitions. They studied DoS vulnerability types under three types: dos-flood, dos-malform, and dos-release, whereas we collected all DoS vulnerabilities in one type. Our trend result highlighted the importance of DoS vulnerability because of its high frequency.

3) They analyzed the frequency trends from three angles: overall trends, OS vs. non-OS vendors, and open vs. closed sources. However, we focused on the overall vulnerability frequency trends and the associated severity.

III. Methodology

A. Data Collection

Data for the period of 2007 to 2010 was extracted from the NVD [3]. This vulnerability data was then sorted by frequency, severity and CVSS base metrics. We referenced the research by S. Christey et al., titled "Vulnerability Type Distributions in CVE" [2]; fourteen vulnerability types were selected based on the frequency. The CSRF vulnerability type was added to the data set due to its importance. It reported less than 0.1% in 2006 and was termed a "sleeping giant" by J. Grossman [4] as it is currently difficult to detect

978-0-7695-4578-3/11 $26.00 © 2011 IEEE
DOI

automatically. Therefore, the true incidence of CSRF vulnerability is likely far greater than reported.

The vulnerability types of CVEs were first selected based on the CWE weakness types which were mapped to the NVD. The CWE is a software community and a formal list of software weaknesses. Its definitions and descriptions support the finding of these common types of software security flaws in code prior to fielding [5]. The NVD uses CWE as a classification mechanism that differentiates CVEs by the type of vulnerability that they represent [6]. From the NVD mapping with the CWE, we gathered 10,068 CVEs which represents 44% of all CVEs for the period under investigation.

When we gathered the CVEs from the CWE-ID, we reviewed their descriptions and found that 75% of the descriptions have similar structures. We also realized the name of the vulnerability type can be found in the explanation. The keyword of the summary is the second step to decide the vulnerability types of the CVEs. In the second step, we searched using keywords from the description to further filter the remaining CVEs. The majority of the keywords are found in the beginning or middle of the descriptions.

Once step one and two were completed to gather and sort the data, we allocated the vulnerability types to the rest of the CVEs from their references. One of the references of CVE is the Open Source Vulnerability DataBase (OSVDB) [7] which offers the attack types, CVE-ID and the attack type of vulnerability. We looked for the CVEs which did not have assigned vulnerability types, but the attack types are in the OSVDB.

Following the three steps of filtering and sorting the data as we mentioned before, we found that roughly 80% of all CVEs were in the select 15 vulnerability types. We were now able to review the trend of their frequency, CVSS scores, and CVSS base metrics for the four years selected.

B. *CVSS*

The CVSS is an open framework to measure the relative severity of software vulnerabilities. It offers a structured approach by the standardized vulnerability scores and prioritized risk. There are three metric groups in CVSS: Base, Temporal, and Environmental. The metrics, which this paper uses, are the base score provided from NVD data feeds. The aim of the base group is to define the basic characteristics of vulnerability. The base metrics consist of base metrics [8]: access complexity (AC), access vector (AV), authentication (AU), confidentiality impact (CI), integrity impact (II), availability impact (AI).

The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores [9]. These qualitative rankings are simply mapped from the numeric CVSS scores as table I:

TABLE I. CVSS SEVERITY RANKINGS

Severity	Low	Medium	High
Base score	0.0-3.9	4.0-6.9	7.0-10.0

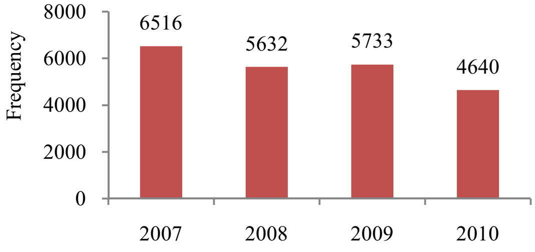

Figure 1. Total number of discovered CVEs

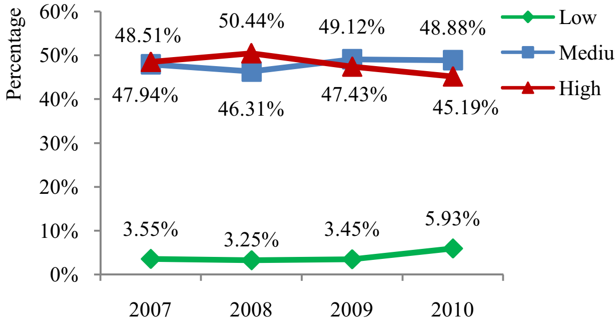

Figure 2. Percentage of vulnerability severity

IV. ANALYSIS

A. *Trend Analysis of Overall Vulnerability Frequency*

Fig. 1 shows all the CVEs frequency distribution over the years according to the published date. The number of vulnerabilities in every year has gradually declined since 2007 and sharply in 2010. It is likely due to secure code practices and software code reviewed in the development. Also, with the marked vulnerabilities decreased, we can assume that CVEs have a backlog which have been disclosed in 2010 and will be published in 2011.

B. *Trend Analysis of Overall Vulnerability Severity*

Fig. 2 illustrates the percentage trends of low, medium, and high severity in each year. Every year, the major vulnerabilities are high and medium severity; low severity vulnerabilities have little presence. The percentage of high severity has reduced since 2008. From that year, the portions of medium and low severity have gradually increased. The severity trend presents the vulnerability distribution in the CVSS scores. In the next section, we will display the trends of base metrics which compose the CVSS base scores.

C. *Trend Analysis of Overall CVSS Base Metrics*

We analyzed the all vulnerabilities from 2007 to 2010 and analyzed trends of CVSS base metrics (AC, AV, AU, CI, II, and AI). The trends revealed the following:

- The frequency of low access complexity has been higher than medium complexity between 2007 and 2009 and lower than the medium complexity in 2010. The frequency of low access complexity has declined by 32% from 2009 to 2010.

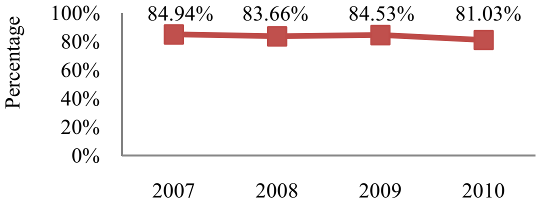

Figure 3. Percentages of vulnerabilities exploited by network access also without authentication

- In Fig. 3, Over 80% of all vulnerabilities were exploitable by network access without authentication in the years we reviewed.
- The CVEs which have partial CIA impacts has roughly 9% increased, and the CVEs which have partial CIA impacts have decreased every year and reduced roughly 12% in the years studied.

D. *Example of a Vulnerability Type Trend Analysis*

We extracted the CVEs of the 15 select vulnerability types, and roughly 80% of all vulnerabilities are involved. The appendix includes these 15 types by severity order (table II) and frequency order (table III). In the select 15 vulnerability types, we also studied the trend of the CVSS base metrics. Due to the page limitation for this submission, we used the DoS vulnerability type as an example to demonstrate the comprehensive trend. The completed trends and graphs of the 15 vulnerability types can be found in [10]. The comprehensive trend of DoS vulnerability type is as follows:

- DoS vulnerability had the third highest total frequency during the four year period. In 2010- in particular- its frequency has been ranked number one among the 15 types. The score of DoS vulnerability has increased from 5.97 (in 2007) to 6.52 (in 2010). The percentage of complete CIA impacts has consistently increased from 2007 to 2010 with a significant increase in 2010. The trends regarding non-confidentiality and non-integrity impacts have been similar, and they have significantly decreased in 2010 (Fig. 4).

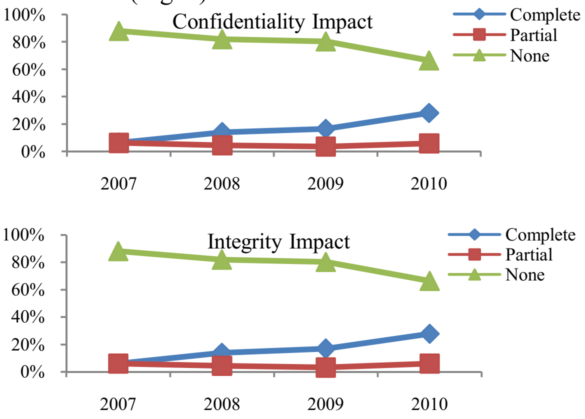

Figure 4. The CVSS base metrics trend of DoS vulnerability type (CI and II)

We can see the various trends from the example of DoS vulnerability type and thus, take the necessary actions to mitigate the vulnerabilities. Our trends of CVSS base metrics in the select 15 vulnerability are upon available request.

V. Conclusion and Future Work

We analyzed the 22,521 CVEs from the NVD for the period 2007 to 2010. All of the CVE data were sorted by frequency, scores, and CVSS base metrics value. There are some significant findings as follows:

- The frequency of all the CVEs gradually decreased, which present positive trends.
- The frequency of high severity vulnerabilities has been decreasing through the years but a portion of it still over 45% in 2010.
- Over 80% of the CVEs were exploitable by network access without authentication from 2007 to 2010.
- The number of vulnerabilities with partial CIA impacts has decreased every year and reduced roughly 12% from 2007 to 2010.
- The percentage trend of complete CIA impacts indicates an approximate increase of 9% for the four years we reviewed.

We further selected 15 vulnerability types from the original data set which contain 18,427 vulnerabilities and their trends have been studied by frequency, severity and CVSS base metric. DoS vulnerability type is an example that we analyzed for the comprehensive trend.

Suggestions for future work include the study of more vulnerability types after 2010 by using similar methodology to analyze the trends. This paper is a contribution to ongoing research in vulnerability trend analysis, which helps the IT professionals to predict threats and protect organizations. Bringing focus on the vulnerability trends, it is hoped that this research will serve as a reference to guide a wide cross section of people in the IT and security field. By analyzing vulnerability trends, IS professionals will be better informed in developing policies that more closely reflect the vulnerability threat landscape. Software developers can use these trends to guide them in development of better coded software, and making them resilient to these vulnerabilities. It is also expected that knowledge of trend analysis can influence the development of security strategies developed by IS professionals.

Acknowledgment

This research was supported by the Concordia Faculty of Professional Education and Faculty of Graduate Studies. The first author wants to specially thank her parents, Chang Chen Hsing and Wang Hong Shi, for their encouragement and support. The first author would also like to thank her colleagues, Boyan Chen, David Edwards, and Luis Perez for their support in number of ways in course of the research.

References

[1] G Stoneburner, A Goguen, and A Feringa, "Risk Management Guide for Information Technology Systems", NIST Special Publication 800-30, July 2002, Available: http://csrc.nist.gov/publi cations/nistpubs/800-30/sp800-30.pdf

[2] S Christey and R. A. Martin, “Vulnerability Type Distributions in CVE”, Common Weakness Enumeration- A Community-Developed Dictionary of Software Weakness Types, May 22, 2007, Available: http://cwe.mitre.org/documents/vuln-trends/index. html

[3] “NVD Data Feed and Product Integration”, National Vulnerability Database, Available: http://nvd.nist.gov/download.cfm

[4] J Grossman, “Cross-Site Request Forgery: The Sleeping Giant”, A WhiteHat Security Whitepaper, July 2007, Available: http://www.whitehatsec.com/home/assets/WPCSRF072307.pdf

[5] “About CWE”, Common Weakness Enumeration, September 26, 2007, Available: http://cwe.mitre.org/about/index.html

[6] “CWE- Common Weakness Enumeration”, National Vulnerability Database, Available: http://nvd.nist.gov/cwe.cfm

[7] “OSVDB: The Open Source Vulnerability Database”, OSVDB, Available: http://osvdb.org/

[8] “CVSS- A complete Guide to the Common Vulnerability Scoring System Version 2.0”, FIRST: Forum of Incident Response and Security Teams, Available: http://www.first.org/cvss/cvss-guide. html

[9] “NVD Common Vulnerability Scoring System Support v2”, National Vulnerability Database, June 20, 2007, Available: http://nvd.nist.gov/cvss.cfm?version=2

[10] Y. Y. Chang, P. Zavarsky, R. Ruhl and D Lindskog, “Trend Analysis of Common CVE Vulnerability Types”, Concordia University College of Alberta, May 2011.

APPENDIX

The vulnerability types in Table |II depicts the severity rank of these select 15 vulnerability types. The rank is listed from high to low according to the average of CVSS scores in the period four years. Table III is ranked by total number of vulnerabilities in the four years. Each vulnerability type includes the frequency, percentage for each year, and percentage change from the previous year. The vulnerability types which have the top five frequencies for that year are represented by (N), which is the rank in front of the numbers that reveal the frequency.

TABLE II. SEVERITY ORDER OF 15 VULNERABILITY TYPES

Rank	Years Vulnerability types	2007	2008	2009	2010	Average
[1]	Buffer overflow	7.98	8.42	8.54	8.44	8.35
[2]	Integer overflow	7.65	8.06	8.01	7.97	7.92
[3]	Format string	7.36	7.15	7.73	7.58	7.46
[4]	PHP remote file inclusion	7.45	7.79	7.26	7.13	7.41
[5]	SQL injection	7.43	7.38	7.36	7.43	7.40
[6]	Authentication	7.46	7.4	6.97	6.79	7.16
[7]	Directory traversal	6.48	6.49	6.49	6.44	6.48
[8]	Denial of Service	5.97	6.15	6.13	6.52	6.19
[9]	Privilege action	6.18	6.59	6.16	5.78	6.18
[10]	Cross-Site Request Forgery (CSRF)	5.8	5.72	6.62	6.39	6.13
[11]	CRLF injection	6.91	5.34	6.64	3.94	5.71
[12]	Race condition	5.48	6.38	5.7	5.09	5.66
[13]	Cryptographic error	5.36	5.36	6.05	5.67	5.61
[14]	Information leak/ disclosure	5.48	4.97	4.87	4.35	4.92
[15]	Cross-Site Scripting (XSS)	4.66	4.23	4.21	4.13	4.31

TABLE III. FREQUENCY ORDER OF 15 VULNERABILITY TYPES

	Years	2007	2008	2009	2010	Total
Rank	Frequency Vulnerability	6516	5632	5733	4640	22521
[1]	SQL injection	(4) 687 10.54%	(1) 1090 19.35% 58.66%	(1) 948 16.54% -13.03%	(4) 515 11.10% -45.68%	3240
[2]	Cross-Site Scripting (XSS)	(1) 824 12.65%	(2) 790 14.03% -4.13%	(2) 821 14.32% 3.92%	(2) 594 12.80% -27.65%	3029
[3]	Denial of Service	(3) 793 12.17%	(3) 597 10.60% -24.72%	(3) 689 12.02% 15.41%	(1) 678 14.61% -1.60%	2757
[4]	Buffer overflow	(2) 812 12.46%	(4) 576 10.23% -29.06%	(4) 571 9.96% -0.87%	(3) 541 11.66% -5.25%	2500
[5]	Privilege action	208 3.19%	(5) 440 7.81% 111.54%	(5) 437 7.62% -0.68%	(5) 350 7.54% -19.91%	1435
[6]	Directory traversal	340 5.22%	353 6.27% 3.82%	319 5.56% -9.63%	273 5.88% -14.42%	1285
[7]	PHP remote file inclusion	(5) 684 10.50%	154 2.73% -77.49%	128 2.23% -16.88%	72 1.55% -43.75%	1038
[8]	Information leak/ disclosure	172 2.64%	222 3.94% 28.32%	216 3.77% -2.70%	222 4.78% 2.78%	832
[9]	Authentication	110 1.69%	173 3.07% 57.27%	266 4.64% 53.76%	119 2.56% -55.26%	668
[10]	Integer overflow	109 1.67%	102 1.81% -6.42%	118 2.06% 15.69%	120 2.59% 1.69%	449
[11]	Race condition	67 1.03%	177 3.14% 164.18%	58 1.01% -67.23%	53 1.14% -8.62%	355
[12]	Cross-Site Request Forgery (CSRF)	63 0.97%	76 1.35% 20.63%	113 1.97% 48.68%	76 1.64% -32.74%	328
[13]	Cryptographic error	53 0.81%	59 1.05% 11.32%	110 1.92% 86.44%	90 1.94% -18.18%	312
[14]	Format string	67 1.03%	30 0.53% -55.22%	26 0.45% -13.33%	15 0.32% -42.31%	138
[15]	CRLF injection	34 0.52%	10 0.18% -70.59%	11 0.19% 10.00%	5 0.11% -54.55%	60
Amount CVEs of 15 types in each year		5023	4849	4831	3723	18427
Percentages of 15 types in each year		77.10%	86.10%	84.27%	80.24%	81.82%