Analysis and Research on Security Vulnerability Database

Jing Fang, Yifu Li, Yingbo Li*

National Computer Network Emergency Response Technical Team/Coordination Center of China

Beijing, China

lyb@cert.org.cn

Keywords: Security vulnerability database; NVD; CVE; Vulnerability; Network Security

Abstract. In recent years, computer viruses, Trojans, worms and hacker attacks are becoming increasingly popular. It has caused certain harm to the political, economic and social world, and poses a serious threat to the Internet and the national critical information system. The vast majority of the security threats are caused by the security vulnerabilities in the system or software, resulting in an endless stream of security incidents. The study of computer system security vulnerabilities and the construction of the vulnerability database is very important for improving the system security and reducing the occurrence of security incidents. The current status of the security vulnerability database is studied, the domestic and foreign famous vulnerability database is analyzed, a study of foreign security vulnerabilities development experience is made, as well as several ideas about the development of the domestic security vulnerability database is proposed.

1 Introduction

Vulnerability is defects which information technology, information products, information systems produced intentionally or unintentionally in requirements, design, implementation, configuration and operation, these defects exist as different forms in information system, once exploited by malicious subjects, it will cause a damage to the security of information system, thus will affect the normal service operation constructs on the information system, and endanger the security of information systems. Such as Ctrip Vulnerability event in 2014, which resulted in Ctrip secure payment log can be traversal downloaded, and a large number of users bank card information leakage. The Heartbleed vulnerability happened in April 2014, which had the most extensive impact in recent years, involving the major online banking, portals, etc., can be used to steal sensitive information server, and capture user's account password on real-time. During the period of being disclosed to repaired, there have been large number of hackers launch a large number of attacks by exploiting OpenSSL vulnerability, some websites information may have been illegally obtained by hackers. Thus, the vulnerability can pose a serious threat to the national political, economic, social harm, Internet and the country's critical infrastructure.

Vulnerability database is the core of network security risk analysis, collecting and sorting out the information, so building the vulnerability database is of great significance. A reasonable, complete information are favor to provide technical and data support for vendors based on vulnerability discovery and attack protection products; and is convenient to confirm the vulnerability that may exist in the environment of their own applications, so as to take preventive measures on time; as well as is conducive for government departments to make an analysis from the overall analysis the amount, type, threat factors and trend of vulnerabilities from overall level, so as to devise the future security strategies. In summary, Vulnerability database relations national security, countries around the world have paid great attention to the construction of vulnerability database.

2 The Current Situation of Foreign Security Vulnerability Database

The research investment of security vulnerability database is earlier in developed countries like Europe and the United States, Domains like Vulnerability mining, classification, rating and other areas is more thorough, so that some industry's influential standards is formed, which has laid a

solid foundation for the development of the security vulnerability database. After several years of development and improvement, some foreign information security agency (security information provider, SIP) has already had deep qualifications and experiences in the construction of vulnerability database, and a group of international influential vulnerability database is forming, such as the United States Vulnerability Database NVD (National Vulnerability database), famous security organization Security Focus. Aus-CERT in Australia, Secunia in Denmark, VUPEN in France.

The United States always keeps a leading place in the field of information security, the PA (Analysis Protection) concerning operating system protection has already started as early as 1970s, and the RISOS (Research in Secured Operating Systems) plan was also carried out. In 1980, the University of Michigan, U. B.Hebbard group had successfully found some vulnerabilities in computer system program through "penetration analysis" (penetration) analysis method, In 1990, the rian Marick B of University of Illinois in the United States made a statistical analysis of the characteristics of the software vulnerabilities. In 1993, the United States Naval Research Laboratory first introduced the concept of time and space in the classification method. Since then, COAST Laboratory of Purdue University proposed a more complete model of vulnerability classification.

2.1 NVD of United States Vulnerability Database

The security vulnerability management was an important part during several periods in United States, an open and flexible vulnerability collection and release and other management mechanism was constructed, as well as the largest vulnerability database was operated. NVD (National Vulnerability Database) was established by the Computer security resource center in United States national standards and Technical Committee, and was supported by Homeland Security National network security division. Vulnerability database includes security vulnerability, related software errors, configuration errors, related products and damage measurement, etc. and also has a high quality vulnerability resource, which is an important platform for vulnerability release and security warning, and is a synthesizer in the field of vulnerability database, both NVD and the academic, industry circles keeps a high cooperation, thus, the vulnerability data is widely used in security risk assessment, terminal security configuration inspection and other fields, which will pay a great contribution for the national information security.

The U.S. national vulnerability database has the following characteristics:

Firstly, vulnerability database has authority in structure specification, information release. the "universal vulnerability disclosure" (CVE) is strictly used in the Naming Standards, that is to say, all the vulnerabilities have CVE number, vulnerability assessment comply with the "common vulnerability assessment system" (CVSS); vulnerability Classification is in accordance with the "common defect enumeration" (CWE), vulnerability database structure and the full support of the standard is the basis of data share, circulation and application.

Secondly, the rich data resources, detailed description of vulnerability. Each vulnerability clauses contains property like number, CVSS score, the complexity of the attack and etc. The perfect vulnerability data has provided support for eliminating the hidden danger, which played a very good role in security warning.

Thirdly, a powerful statistical function is provided. a variety of vulnerability database query can been accessed in United States. The number and trends of various types of vulnerabilities in the historical period can be easily accessed.

Fourthly, the U.S. national vulnerability database remains open. The vulnerability data of XML format can be downloaded, data contains all the information released on the website. Based on standard, normative vulnerability data, the relevant personnel can easily carry out second times according to their own needs.

Finally, the deep application in different aspects, which not only plays an important feature of the release, but also integrates other aspects of the national information security, so that the vulnerability library has played an great role. Such as the security content automation protocol (SCAP) is a method for automated vulnerability management and measurement, as well as compliance assessment by using safe and secure protocol.

In addition to the U.S. national vulnerability database, the United States also has other influential large international vulnerability database, like US-CERT Vulnerability Notes Database, Open Source Vulnerability Database(OSVDB), Security Focus Vulnerability Database located in US-CERT in computer network urgent heart etc..

2.2 general vulnerability disclosure CVE

Most security tools include system security vulnerability database. But there are also differences, which cannot be unified when different databases point to the same question, therefore caused the potential differences in the existence of security coverage, and the different databases and tools cannot be used effectively. In addition, the number of security vulnerabilities are represented by different standard that used by different security tool manufacturer, which means that a standardized specification has not been formed in tool assessment.

This problem was solved by “Common Vulnerabilities and Exposures” MITRE company established, CVE provides a standard for evaluating tools that can communicate with each other in the database and tools, and can accurately know the extent of the security coverage of each tool, which means that the effectiveness and adaptability of the tool can be judged. In short, CVE compatible tools and databases will provide more good coverage, more likely to interact and strengthen security.

CVE is an open and collaborative discussion results. The editorial board first determined whether we should join CVE, then determined the general name, description and reference. The process was like this: firstly found a potential security vulnerability, and then CVE candidate index was distributed by the CVE candidate selected number (CNA) authority, and submitted to editorial board member by editor. The editorial board discussed the candidate and vote on whether it should be the CVE clause. If the candidate was rejected, then the reasons for rejection would be published on Web site in the CVE. If the candidate is accepted, it would be added to the CVE as official clause and published through CVE.

The advantage of CVE is the well-known security vulnerabilities standardization, so that data share and searching will be more easier among different vulnerability database and security tools, the system security vulnerability database structure model and the vulnerability information is constructed based on such advantage.

2.3 Microsoft security bulletin board

Microsoft security bulletin board and Microsoft security recommendations includes a large amount of information security vulnerabilities, which is the most authoritative and detailed information source that user access related vulnerabilities of Windows operating system and Microsoft application. Microsoft security bulletin tells user which vulnerability will cause damage to software or components, what extent of harm will cause, as well as which patch will avoid this damage.

Microsoft security bulletin has the following characteristics:

Firstly, it includes a large amount of information. There are a number of security vulnerability information related to Microsoft included in Microsoft security bulletin, the harm may be caused and the reason came into being will be described in detail in each security bulletins, a specific temporary solution and formal solutions will be given as well.

Secondly, it is authoritative. Microsoft Security Center Web site is the most authoritative website, and is the most reliable source of information for Microsoft products users. Microsoft's security center web site not only is the official agency for releasing security issues, but also is download site for security patch. The relevant information can be found on this site.

Finally, it includes reliable security patches. The best way of solving security problems is to download security patches and update software. Microsoft's security bulletin provides a temporary and formal solution aimed at security vulnerabilities, the temporary solution will be published before the formal solution is proposed, in addition, the security patch can be downloaded and the product can be updated for Microsoft product users.

However, Microsoft security bulletin lacks certain timeliness. As for vulnerabilities, we need to know the trend of the vulnerability on the first time, Timeliness of vulnerabilities is very important.

However, considering security, Microsoft Security Bulletin released regularly once a month, usually it will not be published when the patch has not yet developed previously, so updating vulnerability is relatively slow.

2.4 Experience of foreign security vulnerability development

During a long period of development, foreign security vulnerability database has formed a sound system, from the above analysis, we summed up the following experience:

First is to develop a unified vulnerability standard. A unified vulnerability standard is the basis for circulation and application of the vulnerability information. A number of foreign vulnerability database in different agent have its own characteristics, but they are consistent with or cross reference of CVE standard. For example, the U.S. national vulnerability database comply with a great number of vulnerability standard construction, the authority of the data information is of great value.

Second is to strengthen the construction of vulnerability database data resources and work together. Foreign vulnerability database is widely used in various fields of national information security domain, government departments, security organization, business companies performs its functions and cooperate well, each agency maintain a high degree of information share, various vulnerability database is complementary to each other, thus a complete system is formed. Each domain helps to meet each other's needs, so that provides a strong support for tools and services grouped around vulnerability.

Finally, the construction of the vulnerability library is not isolated, various field cooperation is much needed. Because of mature research of vulnerability mining, vulnerability verification, vulnerability standards, all fields are mutually supporting and promoting.

3. The domestic security vulnerability database development

The domestic research of vulnerability database is relatively slow, which began early in research institutions, some researchers engaged not in collecting and releasing information, but in designing reasonable and perfect vulnerability structure through integrating vulnerability attribute, so this kind of vulnerability library does not put into practical applications. But it has developed rapidly in recent years. Especially in 2009, China's vulnerability database construction work has been a made a breakthrough. There are vulnerability database like national vulnerability database, national information security vulnerabilities sharing platform etc. one after another, which has aroused strong repercussions in the security domain, China has paid more attention to vulnerability database construction.

With the development of information security, some government agencies, security groups began to construct own vulnerability database. The vulnerability database is built on the basis of their own needs, each has its emphasis, but compared with the developed countries in Europe and the United States, there is still a big gap need to be discovered and studied in time.

3.1 National vulnerability database

China's national vulnerability database carried out in October 18th, 2009, vulnerability analysis and risk assessment services are launched out. National vulnerability database is supported by national special funds, and constructed by information security assessment center. After being put into operation, it began to provide analyze and risk assessment service for government agency, industry and society, aiming at improving the ability of national information security threat response and risk management.

National security vulnerability database involves nearly ten thousand kinds of software and products, the main streaming applications, operating systems, and network devices are included. The domestic wide range of application systems, software vulnerabilities are particularly concerned, through the ability of respond to information security threats and risk management level, vulnerability collection, analysis, reporting and oriented to application are greatly improved. National security vulnerability database provide detailed vulnerability information to help users locate and fix vulnerabilities, the key information include software version, vulnerability threat, whether to remote use and corresponding solutions, etc..

3.2 NSfocus vulnerability database in Chinese

NSfocus Chinese security vulnerabilities library is currently the largest number of domestic vulnerabilities, the fastest update vulnerability database, NSfocus Chinese security vulnerability database has become the most well-known vulnerabilities library in secure domain. The content can be summarized, updated and collected on time, the latest bulletin can be released on time, the information release speed is fast.

3.3 Venus Chinese Security Bulletin Library

Venus is one of the most earliest domestic merchant, Chinese security bulletin board system not only completely complied with Chinese standard（ CNCVE）, but also are compatible with the international CVE standard, the database contains large number of vulnerability information, as well as patch information and verification tools, which is the most authoritative information management and retrieval system. By making use of kinds of vulnerability information, the methods and means of hacking can be understood, but also able to make an analysis of the relationship between technical vulnerability that hackers may use and behavior patterns in depth, protecting and tracking the invasion, During the emergency treatment, this tool library not only can analyze attack form and understand attack information, but also can carry out the corresponding protection.

Venus's vulnerability bulletin contains different vulnerabilities, including kinds of operating system and vulnerabilities, bulletin content is quite complete, the information described is very comprehensive.

3.4 Deficiencies of domestic security vulnerability database

As can be seen from the above analysis, although some achievements have been made in the construction and management, some prominent issues are following:

Firstly, lack of a unified standard. At present, there are not standards published related to vulnerability, there are obvious differences in current domestic vulnerability database, there are serious inconsistencies among vulnerability identification, description, classes and rating methods, many terms are Vague, which is difficult to understand, resulting in potential differences in security coverage, and different databases and tools cannot use effectively, which are easy to cause misunderstanding among users, as well as create obstacles to information share and circulation.

Secondly, the released vulnerability clauses also have a certain gap between foreign countries. As the domestic technical capabilities in the field of vulnerability mining is relatively weak, vulnerability clauses are relatively less, the domestic vulnerability database has a considerable proportion of vulnerability information is quoted from foreign countries, the first release vulnerability ratio is less, and domestic software vulnerabilities are also less.

Thirdly, the linkage system is not perfect among various departments. Although cooperation among government agencies, security organizations and business companies, roles and functions are not clear, cooperation is not enough, which cannot achieve a seamless connection, and play the maximum effectiveness of the vulnerability database.

4. Enlightenment of vulnerability database

From the view of politics, standard and technique, Chinese vulnerability database development still has a long way to develop, the development of the domestic vulnerability database suggestions are as following:

First is to accelerate the national standard publication, making compatible with the international vulnerability database. It is specified and standardized data that can share and circulate among different vulnerability database and security tools, and of great value. The classification of the system security vulnerabilities is a special feature of different levels of abstraction. Some systems are classified on the basis of security vulnerability, and some security event management method must be formulated according to system security vulnerability, thus, a set of perfect system security vulnerability classification standard is the foundation. Government departments should take the following situation into account, the number of domestic software vulnerabilities increased year by

year, the rapid development of the software industry as well as part of the domestic software vulnerability has not been included in the CVE standard when draw up the national standard, the national security vulnerability database is designed to support both international and national standards. So accelerating the construction process of the national standard vulnerability database, making all kinds of vulnerability database integration and unity to facilitate the further development of the domestic vulnerability database.

Second is to promote technical research and pay attention to personnel training. China should increase the investment in the field of vulnerability research, establish own talent team, improve China's vulnerability discovery, verification, emergency response ability. Especially in recent years, domestic software security issues becomes increasingly grim, but the vulnerability database collection and publication of vulnerability patch is less, all of this has forced the vulnerability study to an urgent agenda.

Third is clarifying the roles and functions of all agencies. The government plays an important role in vulnerability construction, on the one hand, strengthen unified coordination and management on the national level, at the same time should cooperate with security organizations, business industry companies, security organizations are an important source of vulnerability information, which should give full play to its own technical advantages, pay attention to technical research and cooperation, the research result should be shared with government and business companies, business companies is oriented to users, manufacturers should communicate regularly with government agencies and security organizations to maintain a high degree of sensitivity, provide solutions and response on time. Only to carry out extensive, thorough and effective cooperation, the vulnerability database system will be more perfect and flexible.

5. Conclusion

In recent years, computer network plays an important role in modern society; the construction of vulnerability database has attracted people's attention. Vulnerability database construction is a long-term, full range, multi-level work, research on it will be benefit for preventing system security incidents, reduce the incidence of attack by hackers, exploring the unknown vulnerability. The domestic and foreign development of vulnerability database at present is described, the mature experience of foreign countries is analyzed and summarized, and some useful suggestions are put forward. Establishing a perfect standard system security vulnerability database, making it become the bridge of government departments, social organizations, enterprises and institutions, security companies and the majority of users of the bridge, will be very conducive to the development of national information security. But it is a long and arduous task to study the basic theory of security vulnerabilities, and still need to continue to work hard.

References

[1] NVD(National Vulnerability Database). http://nvd.nist.gov/.

[2] CVE(Common Vulnerabilities and Exposures). http://cve.mitre.org/.

[3] Yu Zhai, Yuqing Zhang, Weishan Wu, Jianwu Hu, Research of System Vulnerability and Database Implementation. Computer Engineering[J]. Vol.30,No.8,2004.

[4] Tom Gallagher,Bryan Jeffries,Lawrence

[5] Landaucer write, Li Zhong, Min Zhu, Jinyong He translate. Track of Security Vulnerabilities. Beijing. Electronic Industry Publishing House. 2008.

[6] Xin Zhao. Vulnerability Attack Technology and Database design[D]. Beijing. Beijing University of Posts and Telecommunications, 2008.

[7] China National Information Security Vulnerability Database[EB/OL].http://www.cnnvd.org.cn/.

[8] China national vulnerability database of

[9] information security [EB/OL]. http://www.cnnvd.org.cn/.

[10] Weili Zhang, Tao Wang, The Situation and inspiration of Europe and the United States Information Security Infrastructure.[J]. Free talk of Network. No.(07)85-89,2015

[11] http://www.venustech.com.cn/Safe/124/.

[12] China Internet Information Center.《Investigation Report of China Software》,2013.