ISSN:0975-9646

Tina Sebastian et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1207-1209

International Vulnerability Database Alliance as an Effective Vulnerability Disclosure Technique

Tina Sebastian[1] Abey Abraham[2]

[1]*PG Student* , [2]*Assistant Professor*
Rajagiri School Of Engineering And Technology

***Abstract*: Vulnerability is one of the key factors that cause security incidents and has become a major international threat to network security. Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability disclosure or the disclosure of a vulnerability is the revelation of a vulnerability to the public at large. Previous work like Common Vulnerabilities and Exposures (CVE) offered to manage vulnerability. However, it had significant disadvantages in coverage and regional differences. The mechanisms of vulnerability disclosure in non-English speaking countries are less developed than the ones in English-speaking countries. International Vulnerability Database Alliance (IVDA) is proposed as an alliance model which consists of security organizations from different countries. IVDA provides an open channel for security organizations to share their efforts across the world. The evaluation of IVDA shows that the international alliance is rational and effective in vulnerability disclosure.**

Keywords-Network Security, Vulnerability, CVE,IVDA

I. INTRODUCTION

Security vulnerability is extremely important for network security. If vendors release patches for vulnerabilities promptly after discoveries, attacks using vulnerabilities will surely affect less number of systems [1]. A security patch is a change applied to an asset to correct the weakness described by a vulnerability. This action will prevent successful exploitation and remove or mitigate a threat's capability to exploit a specific vulnerability in an asset. Security patches are the primary method of fixing security vulnerabilities in software. However, they cannot ensure to produce prompt patches for all their products [2]. Attempts to resolve this dilemma have resulted in the development of vulnerability disclosure [3]. Common Vulnerabilities and Exposures (CVE) was used for vulnerability disclosure. Many databases have included CVE, which is designed to deal specifically with the diversity in identifiers [4]. CVE is designed for providing a common identifier to identify vulnerabilities in different databases. However, given that they are designed for vulnerability disclosure in English speaking countries, the scope of these methods are limited and cannot match the evolving reality of international security vulnerability [8].

CVE allows sharing a lot of data across separate databases and services but it has a lot of limitations [5]. The International Vulnerability Database Alliance (IVDA) will address these maladies. IVDA involves security authorities and combine public resources so as to ensure stable data feeds. We present the basic idea for identifying vulnerabilities of software in different language by providing International Vulnerabilities Description (IVD), which has two status tags and rational management. IVDA systematically extract minimum description fields that IVDA members will include in their vulnerability reports, and provide a general procedure in vulnerability disclosure that brings few changes in the original routines of IVDA members .

The rest of this paper is organized as follows. Section II introduces architecture of IVDA whereas Section III shows the implementation of IVDA. Section IV, compares IVDA with previous work and is shown in Table II. Section V describes the disadvantages of IVDA, while Section VI presents the conclusion and future work.

II. ARCHITECHTURE OF IVDA

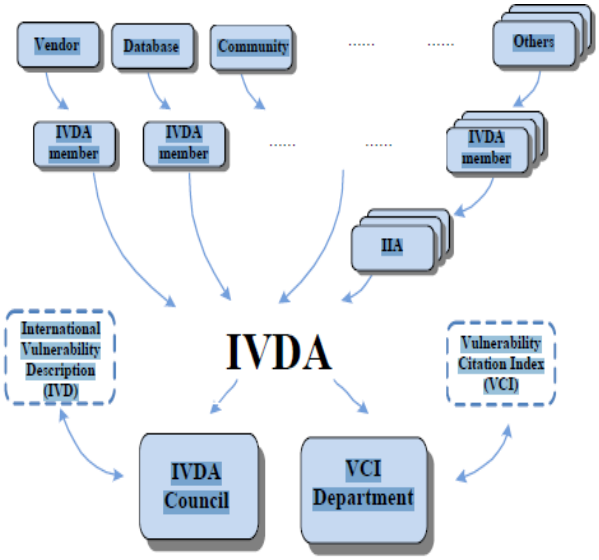

Figure 1. IVDA Architecture

IVDA endorses all the security organizations, software vendors, vulnerability databases and communities to participate in the alliance. Four major roles that will be involved in IVDA are presented in Fig.1, including IVDA members, IVD Identifying Authorities (IIAs), IVDA Council, and Vulnerability Citation Index (VCI) department.

IVDA members are the most basic component of IVDA, which consist of security organizations from different countries. With coordination and communication, they share their efforts and participate in all the work provided by IVDA.

IIAs are some qualified IVDA members, who involve in the policy decision and will be responsible for IVDA. IIAs

are mainly composed of software vendors, and they are allowed to assign IVD identifiers to vulnerabilities of their own software.

IVDA Council is a decision-making section that maintains the normal operation of the alliance. IVDA Council formulates general policies, audits qualifications of IIAs, verifies reports from IVDA members, maintains IVD identifiers and handles duplicate identifiers.

VCI department is dedicated to maintain VCI relying on the reports from IVDA members.

III. IMPLEMENTATION OF IVDA

The actual implementation of IVDA is a phased process that needs data feeds, standard regulations and support of all the other security organizations. The implementation begins with the primitive accumulation of the existing vulnerability data. The data is then processed into a common format, and is indexed in VCI, which is available on internet with IVD. After data accumulation, IVDA invites security authorities from different counties to participate. As IVDA members, they not only provide stable data feeds, but also expand the influence of IVDA by including IVD identifiers in their advisories. With scale spreading gradually, IVDA Council will be in charge of all the routine work. Eventually, IVDA along with all its members will be dedicated to the IVDA issues to ensure this open environment. Standards, policies and regulations provided by IVDA Council will also be improved to match the evolving reality.

IV. COMPARING IVDA WITH CVE

IVDA members announce the vulnerability instantly as they receive the vulnerability reports from researchers. They don't have to wait until the patches are released. The time cost in vulnerability disclosure is reduced to the minimum.

In contrast to CVE, IVDA involves more partners to participate in the alliance and requires multiple vulnerability data exchanges.

Vulnerability disclosure in IVDA is much more consistent and timely, because all the vulnerabilities in an IVDA member include general description fields and have been verified for several times.

Additionally, as the IVDA grows large, vulnerabilities of software in non-English speaking countries can be searched in VCI promptly after it announced in their local IVDA members.

Table I: Description Fields Statistics

IVDA members	NVD	X-Force	OSVDB	Vupen
>=13	17	10	12	17

It can be observed from Table I that vulnerabilities in different databases contain different kinds of description fields. IVDA requires its IVDA members to disclose vulnerabilities covering thirteen basic fields, which provide comprehensive description for vulnerability. With these description attributes, formalized data can be easily obtained by automatic tools and help a lot in further verification by IVDA.

Advantages of IVDA while Comparing with CVE and famous vulnerability databases :

- The coverage of IVDA is much larger. IVDA aims to identify all the vulnerabilities in different languages, and draws up a plan in VCI to expand the coverage of current vulnerability disclosure. With stable data feeds and rational IVD identifier spanning among countries gradually, IVDA will cover all the public vulnerability across the entire cyber world. IVDA also involves new emerging types of vulnerabilities. In contrast, CVE and most famous security databases mainly concern about the vulnerabilities of software in English speaking countries, and just covered a small part of new types of vulnerabilities [10].
- IVDA endorses all the security databases, vendors and community to participate and sort them by country. In contrast to only fifteen CNAs that CVE supports, IVDA has broader data feeds of potential vulnerability [6].
- CVE needs a year or more to verify some candidate vulnerability [7]. While IVDA allocates the work to members of the alliance to directly verify the potential vulnerability. It vastly reduces the workload of IVDA and the time cost in vulnerability verification.
- The distribution of IVD is strictly controlled by IVDA Council. Only IIAs directly include IVD identifiers in vulnerabilities of their own products whereas the other IVD identifiers are totally assigned by IVDA Council. This management policy reduces the risk of duplicate.
- IVDA ensures the integrity of vulnerability data by the general procedure, and resolves regional differences through efforts in international cooperation [9].

Table II: Comparing IVDA And CVE

Parameter	IVDA	CVE
Coverage	Larger	Smaller
Languages	Aims to identify all vulnerabilities in different languages	Does not cover vulnerabilities in all languages
Emerging vulnerabilities	Involves new types	Not adaptive to new types
Potential vulnerability	Broader data feeds of potential vulnerability	Number of CNAs is limited
Workload	Reduced	High
Time for verification	Reduced	Needs a year or more to verify vulnerability
Duplication	Reduced	Existence of duplicate CVE identifiers is vital

Drawbacks Of IVDA

- IVD duplicate cannot be totally avoided. The basic approaches for handling duplication still need evolving [11].
- Vulnerability disclosure in non-English speaking area is still in the state of immaturity. It takes time to meet the requirements of IVDA.
- IVDA requires all databases to maintain English names for indexing vulnerabilities. However, searching in different languages to obtain relevant vulnerability data is more convenient for native users [12].
- The minimum description fields need to be optimized to distinguish similar vulnerabilities efficiently.

V. CONCLUSION AND FUTURE WORK

The earlier works like CVE was mostly used to manage vulnerabilities in English software, while IVDA is a universal model aiming to contribute to the international network security. IVDA provides an open channel for security organizations to share their efforts across the world. When the alliance is implemented, not only vulnerability will have a common format after the general process, necessary communication will also be satisfied. So vulnerabilities in different languages can be searched either in local databases or through VCI. Vendors and governments can obtain the latest security alerts from IVDA to act in response to prevent secure incidents. The future work on IVDA will focuses on the implement issues, involving expanding IVDA members, optimization of minimum description fields, improving IVD duplicate handling, and the multiple language support in VCI.

REFERENCES

[1] R. McMillan, “Siemens: Stuxnet worm hit industrial systems”, Computerworld, September 2010.
[2] G. Keizer, “Microsoft's bug reports fail to produce prompt patches”, Computerworld, July 2010.
[3] Microsoft, “Software Vulnerability Management at Microsoft”, July 2010.
[4] A. Takanen, P. Vuorijärvi, M. Laakso and J. Röning, “Agents of responsibility in software vulnerability processes”, Ethics and Information Technology, vol. 6, no. 2, pp. 93-110, June 2004.
[5] Internet Engineering Task Force, “RFC 2828 Internet Security Glossary”.
[6] NCNIPC, http://www.nipc.org.cn/
[7] CVE, http://cve.mitre.org/about/faqs.html
[8] P. Mell, K. Scarfone, S. Romanosky, “A complete guide to the common vulnerability scoring system version 2.0”, June 2007. Available from: http://www.first.org/cvss/cvss-guide.html
[9] Q. Liu, Y. Zhang, “VRSS: A New System for Rating and Scoring Vulnerabilities”, Computer Communications, Elsevier, vol. 34, no. 3, pp. 264-273, March 2011.
[10] ISS X-Force, http://xforce.iss.net/
[11] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0744
[12] J. P. Choi, C. Fershtman, N. Gandal, “Network Security: Vulnerabilities and Disclosure Policy”, 2007