IVDA: International Vulnerability Database Alliance

A Response

By Kent Landfield

Director, Content Standards, Architecture and Strategy
McAfee Labs

Overview:

This discussion is in response to a paper[1] presented at the 2011 East-West Cyber Security Conference in London. The paper described a proposal for establishing an International Vulnerability Database Alliance. The alliance's intent is to overcome some of the problems of vulnerability identification and disclosure that exists today.

Introduction:

To begin with, the premises presented in the paper are somewhat flawed. The author seems to ignore the last 12 years of effort that has gone into developing and evolving CVE. There is no question, assertions made in the paper about CVE warrant real discussions on how CVE should evolve. However, the paper seems to indicate we should throw out CVE and start over. The authors essentially are missing the point on what CVE is, what it isn't and what it has accomplished.

First, CVE is an identifier for individual software vulnerabilities which is often used as a cross reference across databases, not a database itself (ala, NVD, OSVDB, X-force, Bugtraq, Secunia, etc.). CVEs don't offer much detail about an issue, compared to an actual vulnerability database record. They only have enough information to identify a single vulnerability from another.

Second, CVE has focused on English based products because for the past 12 years, this has been clear direction and consensus of the security and software industry, as communicated to MITRE via the CVE Editorial Board. English based products, which include Internationalized products written in English based programming languages like C, C# and Java, have and continue to make up the largest percentage of the codebase in production. While there are exceptions to the rule, vulnerability analysis tends to be done best when the analysts have a thorough and native grasp of the language used in a software product.

The proponents of IVDA are correct that CVE has focused on English based products. For vulnerability identification and management to scale to the global and international level, we need centers of expertise for each major language used in programming: English, Spanish, Chinese, French and many others. But this does not argue for replacing CVE within the context

---

[1] *IVDA: International Vulnerability Database Alliance',*
Chen ZHENG, Yuqing ZHANG, Yingfei SUN, Qixu LIU
National Computer Network Intrusion Protection Center, GUCAS

vulnerability identification and management of the English based codebase. Rather, it argues for a) IVDA incorporating and leveraging CVE for the management of vulnerabilities for English based products and b) looking for ways to replicate CVE's success by others who can focus on software based on other languages.

CVE's success in enumerating vulnerabilities in English based products is closely tied to CVE's command of the English language. CVE IDs are produced in two ways. Some are based on vulnerability reports that are published, in English, on the web. These are spidered by the CVE team and processed with the aid of sophisticated English based keyword analytics. Other CVEs get produced when the CVE team coordinates with software manufactures and vulnerability researchers on the responsible disclosure of new vulnerabilities. In both cases, command of the English language is central to CVE's success in assigning IDs for English based products.

Based on this, it is unreasonable to expect CVE to immediately scale globally. More to the point, no single group can be expected to assign vulnerability IDs for all languages, regardless of regionally developed software. The solution is to replicate CVE's success for other languages, not to replace what is working well for English based software.

Weakness of CVE

The paper goes to great length to discuss the weakness of using CVE today. Here is my take on their fundamental concerns:

1. ***CVE doesn't cover all the vulnerabilities.***

    - ***CVE doesn't cover all of the vulnerabilities in English speaking countries***

      This is a true statement. There are a couple of reasons why this is the case. First and foremost is a matter of resources. The MITRE CVE Team who manages the CVEs does not have unlimited resources and as such must target those classes of vulnerabilities that have the most impact on organizations and consumers. This has been a known issue for years. The CVE Team has canvased vendors and the CVE Board to try to understand what are the critical types of issues to cover and what can be bypassed.

      By and large, CVE produces IDs for the English based software that is considered to be the most important by the software industry. If we, as an industry, believe that CVE IDs need to be produced for an even larger percentage of English based software, we should be engaged with MITRE's US government sponsors regarding increased funding to allow for that.

- ***Many software vulnerabilities not in English are not covered by CVE***

  This is also true, but not for the reasons they claim. CVE has been an English focused activity. If nobody alerts the CVE Team to a non-English vulnerability, a CVE won't be created. As stated in the paper, "mechanisms for vulnerability disclosure in non-English speaking countries is less developed than those in the English speaking countries". It's essentially an issue with non-English vendors, vulnerability researchers, and CERT type organizations not coordinating the need with the CVE Team.

  The author incorrectly (to my knowledge) claims that CVE will essentially deny requests from people who are not "official partners". I do not believe this is true. If you have a valid issue, you can submit for a CVE, regardless of the regional attributes for software.

  Reality is, CVE has been developed for users of English based software. It has been funded by different US government agencies throughout the years with the target goal of supporting US vendors and software to be used within the US Federal Government and US industry. CVE matured to where it is today because of the participation by software vendors in accepting CVE and using it to identify, correlate and report on software defects. The development of regional software was not an initial goal of the effort.

  This one issue (non-English vulnerabilities not covered) seems to be the real reason for this proposal in the first place. It is true there are problems with CVE when it comes to language support and in fact this is true for most of the SCAP enumeration standards. Only CPE truly provides language support today.

2. CVE is not adaptive to new types of vulnerability

This is a false statement. CVE is not CWE. It's agnostic to the type of vulnerability submitted. CVEs do however focus on specific software vulnerabilities, and not service vulnerabilities. The CVE Team will include XSS vulnerabilities in a shopping cart that you can download and install, but not one in Amazon's shopping cart, for instance. The authors miss an integral point by implying a general software vulnerability database should include these. There is fundamentally no value for products that are consumers of CVE data to have to assimilate and track XSS service related issues on websites. More often than not, those are exceedingly temporal (fixed in a day), and outside of historical interest, there isn't much use for that data in any way needed to assess or remediate problems on systems you own. And as more cloud services are fielded, you can bet those services will fix security issues quickly if they wish to stay viable as a service.

Regardless, how CVEs are issued and for what types of software vulnerabilities are more a

policy and funding issue and is not an inherent weakness in the structure of CVE and its usage.

3. The number of CNAs is limited

The numbers of CNA are limited to those organizations the CVE Team knows will produce a large number of CVE identifiers and they are issued blocks of CVEs to assign from. McAfee applied for CNA status and we were denied because we publish no more than 10 or so a year. They want organizations that produce 100 or more. This is essentially a time saving concept, not an "exclusive club" of any sort. It is also reasonable to assume CVE's criteria of 100 or more a year is related to funding. CVE wants to maintain strict control of their process, but have developed trusted relationships for which they can offload work closer to those with the issues being reported. If an organization meets the volume criteria, I suspect CVE wouldn't bat an eye at including them.

Secondarily, the existence of CNA organizations does not preclude individuals and non-CNA organizations from submitting at all.

This is one area where changes to the policy and procedures of how CVE is managed could easily solve the author's concerns.

4. Duplicate CVE identifiers

This happens periodically. CNAs should be responsible for their issued blocks. If they are not, it should be handled by the same backend system in a reasonable way. If this is happening, there are reasonable process and technological answers for this.

Today when this occurs, the duplicated record is deprecated so that it is not used again. This approach was decided on over time as the best approach to take. The paper proposes

> IVDA Council takes the following basic approaches to handle duplication and conflict issues in IVD identifiers.
> • If two vulnerabilities are assigned the same IVD identifier, the earlier one's IVD will be reserved, and the later one will be assigned another IVD identifier by IVDA Council.
> • If a vulnerability has two IVD identifiers, the identifier that assigned for the longest period of time will be reserved.
> • If two identifiers are assigned for the same time, the one which is assigned by the original vendor or firstly verified by IVDA Council will be reserved

Except for the first item, there is nothing to say the CVE Team could not take a similar approach. We have determined that reassigning a duplicate CVE can cause confusion due to data inconsistency issues. If someone looks up a CVE that is a duplicate, marks it as such in his or her product or local data, and it is later reused, data inconsistency can occur. If the offending record is taken out of service, this reduces the potential for impact on the end user.

Regional differences in vulnerability disclosure

As mentioned earlier, the author states that the mechanisms of vulnerability disclosure in non-English speaking countries are less developed than those in English-speaking countries. He goes on to state that many software vendors in non-English speaking countries just release patches quietly. He also states vulnerability databases in China were established only recently and the repositories focus on vulnerabilities for Chinese software. I'm uncertain how a new tracking mechanism would help here. I suggest that instead of trying to change CVE, which works well for English based software, we should advocate IVDA focus it's energies on trying to replicate the success of the responsible disclosure movement as demonstrated by CERT-CC and others. From the start and by design, CVE's are assigned to publicly known vulnerabilities. If there were to be better disclosure practices for non-English software, it would be more practical to talk about CVE-like solutions for those markets. Outreach programs that tie people into well-developed processes and procedures already in use seems like a better idea. This could be done from a central organization, or via local partner organizations. The author indicates the NVD only contains a minority of Chinese software vulnerabilities. While I am sure this is accurate, this is a situation that could be remedied with some coordination with the CVE and NVD teams.

Diversity in vulnerability management procedure

The authors are essentially critiquing the fact that different databases contain different information. This is by design. The quantity and quality of a vulnerability database's information is a distinguishing mark. CVSS is standard base score, but if a vulnerability database, or vendor for that matter, wishes to create their own, more meaningful metric of risk, why shouldn't they? Some don't provide much detail on the bug, or the fix. Some actually validate vulnerabilities exist and put real resources behind validation and confirmation of bugs. For example, Secunia often emails McAfee staff after a public disclosure with additional questions. Others are essentially robots, collecting what they need. The author seems to indicate the NVD, Security Focus, X-Force and OSVDB all have the same purpose, reason for being and target audience. This shows a lack of understanding as to their ownership and audience. NVD is the one database that most consider 'official'. Other 'data sources' such as those mentioned above are used for proprietary purposes or 'community projects'. If there were to be an additional vulnerability database (and there are) then vendors and large organizations would simply use them as an additional source to 'mine security vulnerability knowledge' from.

Proposed International Vulnerability Descriptions Identifiers

The authors, after describing all the perceived weaknesses in CVE, describe a new IVD identifier that is to be used in much the same fashion as a CVE. One interesting item is the

format of their proposed IVD is as follows:

> IVD-YYYY-NNNNNN of which YYYY is a decimal digit that represents the year of the vulnerability disclosure and NNNNNN is a 6 decimal digit as the serial number of the vulnerability.

It should be noted that a CVE identifier format is as follows:

> CVE-YYYY-NNNN

So what is the real difference? 2 digits on the CVE identifier... Currently CVE is limited to 9999 CVEs being issued in a single year while the paper's proposal supports 999,999 unique vulnerabilities.

This limitation has been actively discussed in the CVE community and on the Board in the not too distant past. All seem to understand we will need to increase the length as the number of vulnerabilities creep closer to the 10,000 per year mark.

Establishing an International Alliance

For years now there has been a discussion around governance of various security automation standards but at present, no one has been able to come up with a framework that is workable from a national, let alone global perspective. While the US Government is working actively to develop governance for their aspects of the standards and their directional needs, that will not work on a global scale. NIST, NSA and DHS cannot honestly stand as the owners of an international effort of the type mentioned in the paper. It is obvious there is a need to have that type of oversight and management of efforts such as CVE, CCE and others. Besides what is in the paper, I do not know enough of their governance proposal to form an opinion. It is however, just one more piece of evidence other countries are feeling the pain and want to address it. This proposal seems to be open on the surface but this is a proposal from a group that has not been active from a standards perspective in the past so I find it hard to believe they understand how a real public/private partnership would or should work. That does not however diminish the needs they describe.

So where do we go from here?

Good question. Here are my opinions on actions that need to be taken.

First, the proposal identified a few issues that truly need to be addressed in CVE today.

Vulnerabilities do not simply occur in the software produced in English speaking countries. They occur in all software and as such we need to have a means to record when vulnerabilities surface. Products today are sold globally and need to be effective in a global user space. Just because a network or host vulnerability scanner was developed in the US, it should still be just as effective identifying vulnerabilities in regionally developed software as they are identifying vulnerabilities in US developed software.

1. **CVE needs to be able to be internationalized.**

   The supported formats should support Unicode characters. There may be a need to have existing and newly created CVE entries localized in more that just English. This will have to be determined based on multiple considerations. The localization could be done by local partner organizations such as the NCNIPC. Additionally the CVE review team may need translation capabilities to better serve non-English submitters.

2. **CVE needs more outreach**

   This is needed to try and educate the non-English sections of the globe how to work with the established policies and procedures. This could be done by local partner organizations that are supporting CVE submissions in that part of the world. Additional documentation such as Informational RFCs issued through IETF could also assist. RFC-Editor will accept these types of RFC submissions without the need for a working group.

3. **CVE needs to consider refining their CNA status qualifications and procedures.**

   In the past this has been reserved for the Microsofts of the world. As other organizations want to act on the behalf of a nation or region, the CVE CNA authorization process should adapt to provide the legitimate additions to be an active part of the CVE issuance process.

4. **The CVE format needs to be expanded to 6 digits from 4.**

   9999 vulnerabilities in a single year will be quickly exceeded if we are looking to include regional software not developed in English speaking countries. Support for 999,999 vulnerabilities is reasonable for the foreseeable future.

   While this sounds easy, there may be complications as some vendors have hardcoded the existing format into their software or databases. This is one area that may need an impact study before the CVE standard format is enhanced.

5. **If nation states want to establish their own national vulnerability database, they**

should be able to if they wish to fund them.

The question of centralized vs. decentralized storage of CVE related information comes into play here. I suspect certain nations, such as the US would act as aggregators to assure all unique CVEs entries were represented in the US NVD. We should however do nothing to inhibit the capabilities of individual countries to stand up or replicate their own version of the NVD if they so desire.

6. **Existing CVE management processes need to be reviewed.**

   We need to determine which processes may need to change to provide international support of identifying and labeling software vulnerabilities. At the same time the process review needs to determine if there are more effective automated means of handling the load so that more vulnerabilities can be cataloged.

7. **Need to put a long term funding foundation under the security automation standards**

   Regardless of this proposal, we need to assure the critical foundation pieces of the security automation efforts that have been so successful, have a long-term financial foundation if we wish to assure the success of integrated security automation in the future. CVE, CCE, NVD and other efforts are critical to the security industry today. It is very important we provide a means to assure their operational availability and viability for years to come.

Summary

It is obvious identifying software vulnerabilities is a global need. The real question is do we start over with an IVDB and a new IVD identifier, essentially throwing the baby out with the bath water, or do we evolve the existing 12+ years effort that has a foundation in most security vendors products, databases and documentation? I am very biased being an initial and current member of the CVE Editorial Board.

The paper depicted we need to really think globally. This is not something the US government has really had to do until just recently. US vendors have been assuring our products can be sold in a global market space but as a community, based in the US, we have not looked to support the regional needs of locally developed software in other parts of the world. As a community (US government, US vendors) we have repeatedly stated we do not want to do anything that would inhibit global security infrastructure to effectively use our security automation standards

but it seems that we have and now it is time to address it.

If we do not address the concerns and needs communicated in the paper, we could easily find ourselves in a situation where competing standards are established in non-US emerging markets. This would not be good for US vendors and ultimately the US Government if it hopes to be able to continue to have a real say in the directions of the security automation standards in support of its mission.

Governance is an issue that must be addressed and one that may not be able to rely on an existing international organization. If it appears a new governance body for operational based security standards and enumerations is needed, it will be best for all if the US government works with industry to take the lead and not be taken for a ride. Regardless, all apparently will lose some aspects of control while gaining a global foundation for building future security automation and knowledge products from a single standards base.

About the Author :

Kent Landfield is Director of Content Security Standards, Architecture and Strategy for McAfee® Labs. He spent over 25 years in software development, global network operations and network security arenas. He has been involved with the development of security standards since the POSIX working groups in the late 1980s. Landfield has also been involved with standards development for the Trusted Systems Interoperability Group, the Internet Engineering Task Force and Trusted Computing Group. He was one of the initial CVE Editorial Board members and is also an OVAL Board member, a CPE Core Team member and is active in other emerging security automation standards.