CVE/NVD: The High Price of 'Free'

7/6/2015

Richmond, VA

855-RBS-RISK

vulndb.riskbasedsecurity.com

sales@riskbasedsecurity.com

Vulnerability Intelligence (VI) is not a new offering by any stretch of the imagination. However, in the past few years VI has gained more attention and become an integral part of security offerings and the foundation for network defense. While there have been several companies offering VI over the years, one U.S. government-funded offering has erroneously become the defacto standard; I'm referring to the Common Vulnerabilities and Exposures or CVE project run by MITRE. The CVE project calls itself "*a dictionary of publicly known information security vulnerabilities and exposures*" and says it "*is not a vulnerability database*". Rather, CVE was designed to "*provide common names for publicly known problems*" with the design of "[*allowing] vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services*". In spite of CVE's disclaimer, (CVE is not a vulnerability database), its price tag (a freely available resource), make it irresistible to most organizations as a free source for VI. In reality, the price of using CVE as a sole source of VI is incredibly high and growing as evidenced by the increasing number of successful computer-based attacks. There are numerous facets of the CVE offering that are not well known, or perhaps are ignored, which make it inadequate to provide even the most basic vulnerability intelligence. In spite of knowing its severe limitations, CVE continues to pass itself off as "The Standard for Information Security Vulnerability Names". Based on misinformation, CVE's public image, the price tag, or convenience, just about every vendor serving the security industry uses CVE for VI. This includes firewall vendors, IDS / IPS, vulnerability alerting services, those generating vulnerability statistics, and more. CVE has become a cornerstone of the security industry.

The most important thing to understand about CVE is that it simply is not a comprehensive vulnerability database (VDB), or dictionary, and publically states its limitations. While no VDB can honestly claim to cover "all" vulnerabilities, they can certainly make known their mission and commitment to do so. This is done by not only maintaining expert staff to aggregate the vulnerabilities from public sources, but also by utilizing an ever-growing list of sources that contain such information. Until last year, CVE maintained a public list of sources that was virtually unchanged since its inception in 1999. After pressure from the public and the CVE Editorial Board, compromised of non-MITRE industry "advisors", CVE revised their coverage policy and shifted to a new system of 'full' or 'partial' coverage based on the vendor, product, and/or vulnerability source. On the surface, this list looks promising, but upon any significant scrutiny, it

> *Unfortunately, CVE can no longer guarantee full coverage of all public vulnerabilities... we are not well-prepared to handle the full volume of CVEs for all publicly-disclosed vulnerabilities… – Steve Christey, Editor of CVE*

is utterly lacking in adequate coverage. In order to head off complaints, their webpage even qualifies 'full coverage' sources by using the phrasing "*nearly all issues disclosed*" to "*allow the flexibility to potentially postpone coverage of minor issues*".

This statement is entirely misleading as CVE routinely fails to cover medium and high-risk vulnerabilities in the products listed. For example, in 2013, CVE failed to cover 16 vulnerabilities in Microsoft products including one remote code execution vulnerability and three context-dependent (i.e. user-assisted) code execution vulnerabilities (that number jumped to 20 in 2014). Their list maintains they cover Google

Chrome (including the underlying rendering engine WebKit), yet CVE failed to cover 32 WebKit and 18 Google Chrome vulnerabilities in 2013 (27 WebKit and 83 Chrome in 2014). Even before this failure to cover high-priority vendors, CVE had already given up on the illusion of being comprehensive.

When comprehensive vulnerability intelligence is a critical part of an organization's security program, (how can it not be), it is important to understand how comprehensive, timely and high-quality your chosen vulnerability intelligence provider is. These are key metrics that enable you to understand the value provided and ensures that you are receiving the information required to make risk-based decisions about patching and remediation.

With many organizations still spending a fraction of their budget on Information Security, and many companies increasingly cutting those budgets, it is easy to understand the appeal of free vulnerability intelligence. The U.S. government funds several redundant sources of vulnerability aggregation including MITRE's CVE project, NIST's NVD, Carnegie Mellon CERT, and the DHS' US-CERT. While the two CERT bodies do not maintain a comprehensive collection of public vulnerabilities, some organizations rely on them for "high-profile" vulnerability announcements. With only 18 advisories in 2014 covered by US-CERT, that is less than 1% coverage of vulnerabilities disclosed last year, US-CERT can hardly be depended upon as a VI solution.

MITRE's CVE project is the central public government-funded aggregation point for vulnerabilities, which is then shared with NIST's NVD for additional analysis (e.g. adding CVSS and CPE data). While the free CVE and NVD offerings are considered the cornerstone of VI, it is woefully inadequate. Looking at the last five years and the start of 2015, you can see in the table below that CVE aggregates only about 50% of the vulnerabilities that Risk Based Security's VulnDB does.

	2015	2014	2013	2012	2011	2010
CVE Total IDs	1160	9514	7420	6685	5323	5320
CVE Reserved	1098	2697	1765	1514	890	379
CVE Rejected	0	67	106	94	70	47
CVE Live	62	6750	5549	5077	4363	4894
VulnDB Live	791	13129	11116	10390	7967	9207
CVE Missing	729	6379	5567	5313	3604	4313
CVE to VulnDB %	7.84%	51.41%	49.92%	48.86%	54.76%	53.16%

This should be very alarming to any organization who is trying to maintain network and application security. The old adage of "*a hacker only needs one way in*" is put into perspective that should cause alarm. Almost every security device designed to detect and prevent vulnerabilities relies solely on the data provided by CVE / NVD. Missing a single vulnerability can lead to an organization-wide compromise that is costly and embarrassing.

Even worse, the list of sources that CVE uses to aggregate vulnerability intelligence is very slanted toward desktop software and has almost no coverage of third-party libraries. Today's software is a virtual mish-mash of third-party code used to implement standards and save development time. Consider that Adobe Reader, what appears to be simple software for rending PDFs, makes use of over

200 pieces of code that Adobe did not author. Underlying libraries that handle functions such as image rendering (e.g. FFmpeg), parsing web pages (e.g. WebKit), or handle encrypted communications (e.g. OpenSSL) can contain vulnerabilities that manifest in thousands of products.

We've grown up thinking that "the best things in life are free". For drink refills and advice, that notion certainly has merit. When it comes to vulnerability intelligence though, "free" certainly comes with a high price tag.