QuickView
VulnDB

Vulnerability QuickView

2017 Vulnerability Trends

Created by:
Risk Based Security

Issued February 2018

Rise in Vulnerabilities Continues

- There were **20,832** vulnerabilities published by Risk Based Security during 2017, a **31.0% increase** over 2016. This rise was also reflected in the number of vulnerabilities documented by the National Vulnerability Database.
- Risk Based Security's VulnDB published **7,900 more** vulnerabilities than CVE/NVD in 2017.
- CVSSv2 **scores above 7.0 accounted for 39.3%** of all vulnerabilities published in 2017.
- 44.5% of the vulnerabilities not published by NVD/CVE have a CVSSv2 score between 7.0 and 10.
- Coordinated disclosure accounted for 44.8% of the 2017 vulnerabilities.
- Twelve vendors accounted for 54.25% of 2017 vulnerabilities.
- Web-related vulnerabilities accounted for 50.6% of 2017 vulnerabilities.
- 31.5% of 2017 vulnerabilities have public exploits and 48.5% of all disclosed vulns in 2017 can be exploited remotely.
- 24.1% of 2017 vulnerabilities have no known solution.
- At least 5.9% of 2017's public vulnerabilities were coordinated through bug bounty programs.
- 1.7% of 2017 vulnerabilities were classified as SCADA vulnerabilities.
- 28.9% of web-related 2017 vulnerabilities are Cross-Site Scripting (XSS).

Not Just Security, the Right Security.

Introduction to the VulnDB QuickView Report

The amount of activity around vulnerabilities heated up in 2017. The number of vulnerabilities publicly reported or disclosed to companies increased by nearly a third. The majority of the vulnerabilities occurred in web-based software — making up the majority of security issues discovered and reported in 2017.

While many researchers tend to minimize the risk of some web-based attacks, such as cross-site scripting (XSS), they are still an effective attack. The persistent presence and growth in SQL injection attacks – always deemed a severe issue – should be worrisome. Much of the increase may be due to better reporting of vulnerabilities to software developers and companies. The continued migration of applications and functionality to web-based software and services is certainly responsible for much of the increase as well.

The trends in other areas, however, should concern all security professionals. Security software, industrial control software, and programs associated with cryptocurrency are all in vulnerability researchers' crosshairs. Because of its privileged place and access to most networks and data, any vulnerability in security software should be taken seriously. SCADA vulnerabilities continue to attract attention, and with attacks on power infrastructure in Ukraine and the Middle East could be very damaging.

Meanwhile, less than half of all vulnerabilities are being shared with the software developers in a coordinated disclosure process. Software developers rely so much on third-party researchers that they need to make sure that outreach is part of their software-security process.

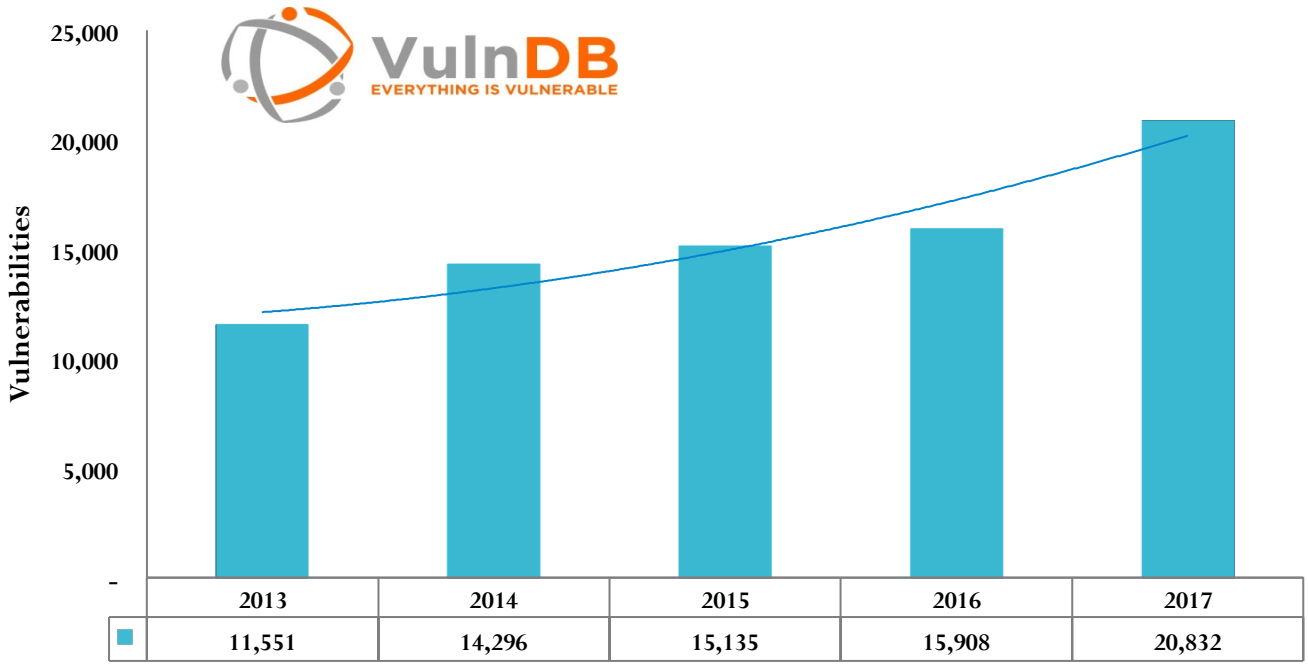
What does this report cover?

This report covers the vulnerabilities captured by Risk Based Security during 2017. The information collected is displayed in a series of charts depicting various groupings, classifications, and comparisons of the vulnerabilities disclosed from January 1st through December 31st of 2017. In cases where prior year totals are shown, as well as the 2017 calendar year, the data is based on calculations made as of January 15th, 2018. This is due to vulnerability databases assigning and/or aggregating data from prior years during the current year. This report is designed to provide a variety of observations around vulnerability disclosures in 2017 that can be referenced in your organization.

If you have any questions or suggestions for the next report, please contact us at support@riskbasedsecurity.com.

We hope you find the report useful!

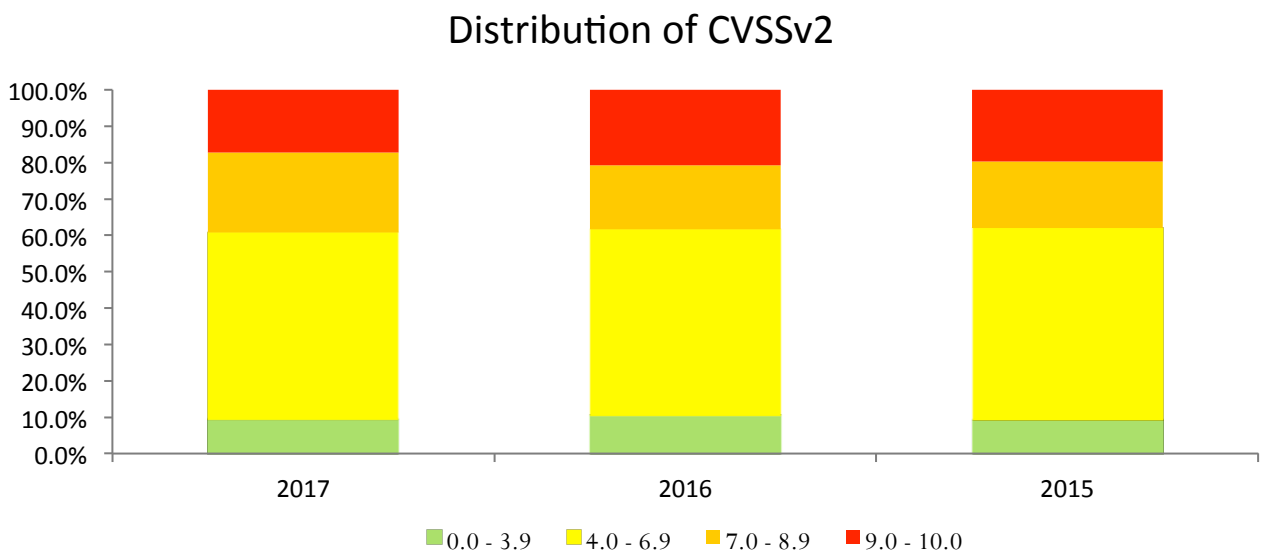
Vulnerabilities Continue to Rise



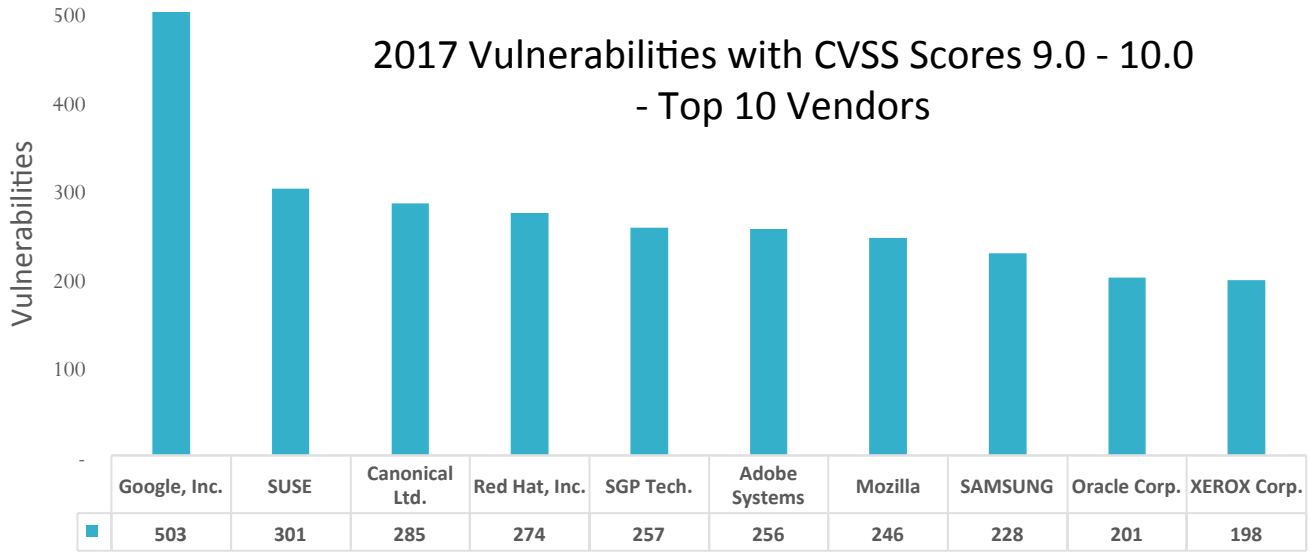
The number of vulnerabilities cataloged by VulnDB during 2017 was at an all-time high. Even the 2,700+ increase from 2013 to 2014 (19.3%) has been surpassed by the number of disclosed vulnerabilities by the end of 2017, **a 23.7% jump from 2016**. As of the release of this report, 2017 is a record-breaking year regarding the number of vulnerabilities disclosed! This means that organizations must not only remain vigilant in patching, but they must pursue their vendors to ensure that security devices are capable of detecting these vulnerabilities. Intrusion Detection Systems (IDS) and vulnerability scanners that are only looking for a fraction of these vulnerabilities will not properly protect your network.

Compared to the same period in 2016, **2017 has averaged 1,736 vulnerabilities per month** compared to 1,289 in 2016, a 34.7% increase. Even with the increase in the number of disclosed vulnerabilities in 2017, it is crucial to remember that the VulnDB research team will continue adding vulnerabilities as they are disclosed from prior months. As such, the 2017 total will continue to grow. For example, VulnDB added 908 vulnerabilities disclosed in 2016 during the 2017 calendar year.

CVSS Comparisons



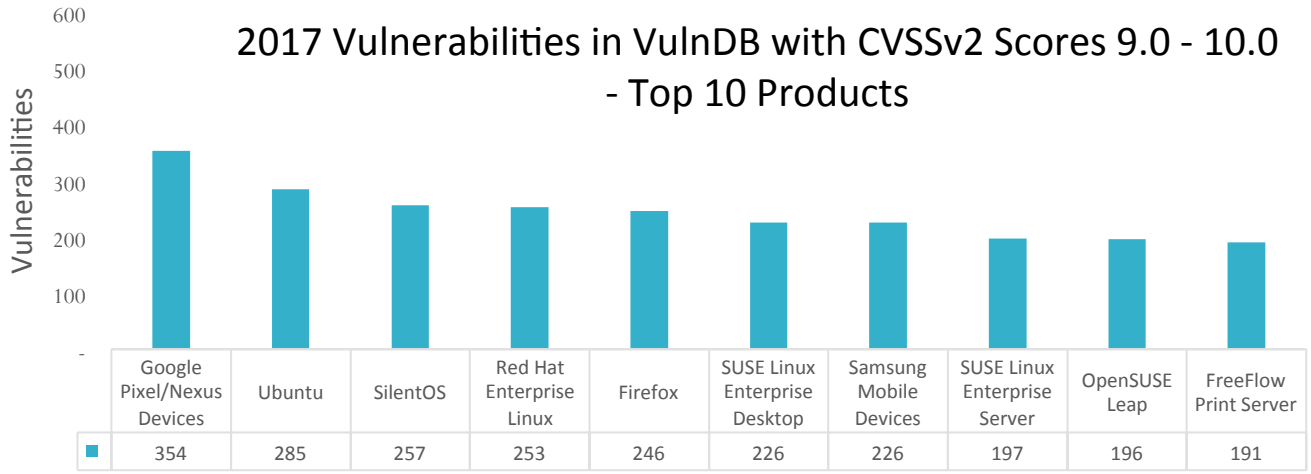
CVSSv2 scores for public vulnerabilities have been relatively consistent with about 40% of the vulnerabilities scoring between 7.0 and 10. With 17.2% of vulnerabilities disclosed in 2017 having a CVSS score between 9.0 and 10.0, organizations must stay vigilant.



Breaking down the CVSS scores further, it is interesting to look at the top 10 vendors with vulnerabilities scored between 9.0 - 10.0. **While you might expect vendors such as Canonical (maker of Ubuntu) and Red Hat to appear on the list, due to their inclusion of a wide variety of software, vendors such as XEROX and SGP Technologies may come as a surprise**. For those unfamiliar, SGP is a subsidiary of Silent Circle, a player in mobile devices and applications.

Note that the numbers reflected in the chart do not necessarily represent unique vulnerabilities in their products. For example, some XEROX products bundle Mozilla Firefox, and a portion of the Google and Mozilla vulnerabilities are in third-party libraries.

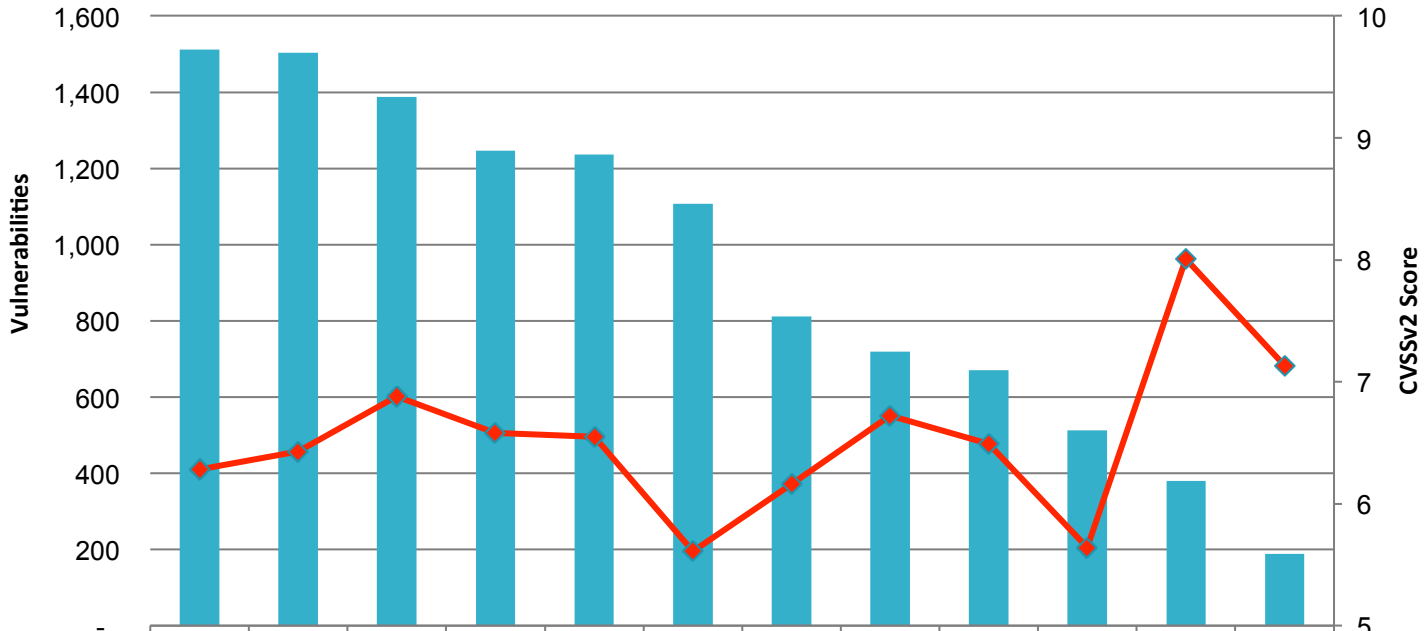
2017 Vulnerabilities in VulnDB with CVSSv2 Scores 9.0 - 10.0 - Top 10 Products



	Google Pixel/Nexus Devices	Ubuntu	SilentOS	Red Hat Enterprise Linux	Firefox	SUSE Linux Enterprise Desktop	Samsung Mobile Devices	SUSE Linux Enterprise Server	OpenSUSE Leap	FreeFlow Print Server
■	354	285	257	253	246	226	226	197	196	191

In conjunction with the vendors above, the vulnerabilities directly correspond to high-deployment products they offer. This shows that products ranging from personal devices such as cell phones (e.g. Pixel, Nexus, Blackphone SilentOS, Samsung) all the way to enterprise operating systems (e.g. Ubuntu, Red Hat Enterprise Linux, SUSE Linux Enterprise Server) have high-risk vulnerabilities that must be addressed.

2017 Vulnerabilities and Average CVSS Scores - Major Vendors

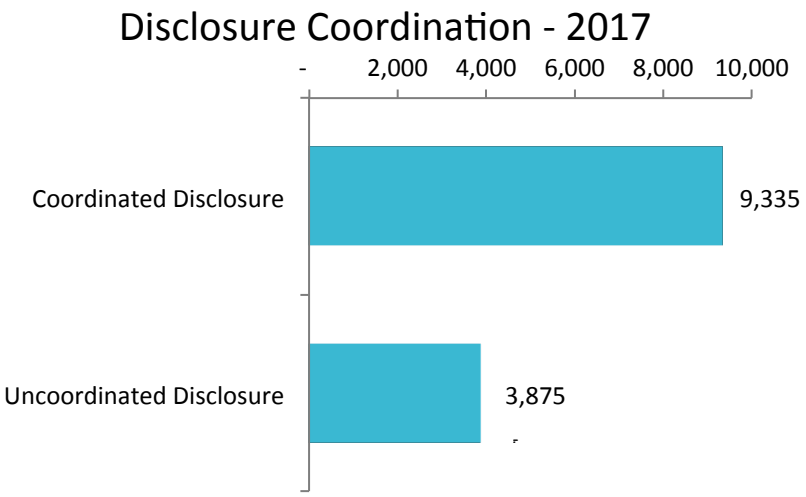


	Oracle	SUSE	Google	Red Hat	Canonical	IBM	Microsoft	Samsung	Apple	Cisco	Adobe	HPE
Total Vulns	1,512	1,504	1,387	1,247	1,236	1,107	812	719	670	512	379	189
Average CVSS	6.28	6.43	6.88	6.58	6.55	5.61	6.16	6.72	6.49	5.64	8.01	7.13

Products from major vendors account for 54.1% of the vulnerabilities reported in 2017. The average CVSSv2 scores for the vulnerabilities for each vendor is in the 'Medium' range. The average CVSSv2 score for vulnerabilities in Adobe and HPE products was 'High'.

2017 HIGHLIGHTS

Disclosure Coordination



At least 44.8% of vulnerabilities disclosed in 2017 were coordinated with the Vendor.

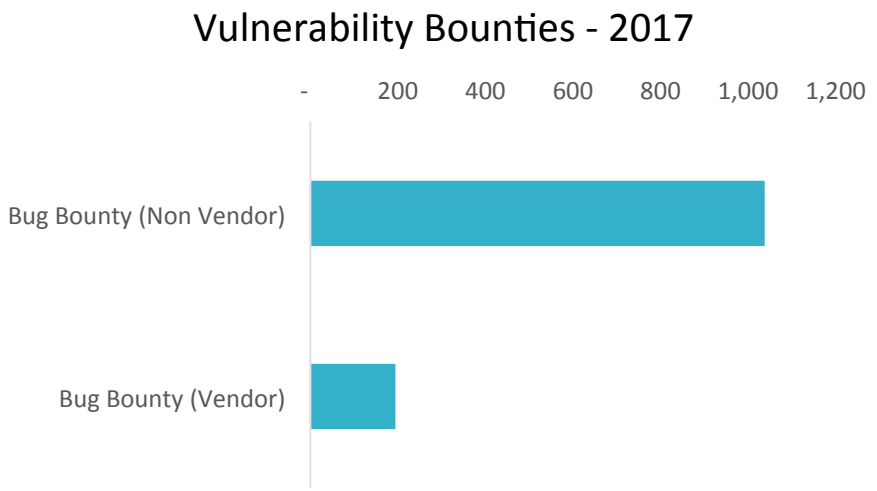
Note that some vendors do not clearly indicate if a disclosure was coordinated. Further, many researchers will attempt to coordinate with the vendor, but find them unresponsive and/or take too long to fix the issue. As such, **despite an attempt at coordination, some vulnerabilities are disclosed before a fix is available**.

Disclosure Coordination Trends

Year	Coordinated Disclosures	Uncoordinated Disclosures
2013	28.1%	20.5%
2014	28.4%	29.2%
2015	40.9%	15.8%
2016	45.6%	14.2%
2017	44.8%	18.6%

An interesting trend over the last few years is the growing percentage of disclosures that are coordinated with the vendor. **Since 2013, the number of coordinated vulnerabilities has increased by 16.7** percentage points based on the vulnerabilities aggregated. One factor in this increase is the rising popularity of GitHub, where users can submit issues to the software vendor/developer directly. While the information is made public right away, many developers do not specify any other method to report an issue, even if it has a security impact. So researchers following the developer's guidelines and reporting issues via the bug trackers is coordinated. This is a good reminder that vendors need to consider a separate reporting mechanism for security-sensitive issues.

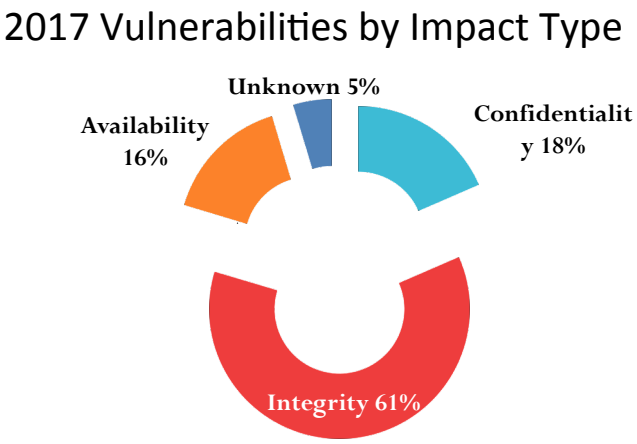
Bug Bounty



5.9% of 2017 vulnerabilities were the result of vendor or third-party bug bounties.

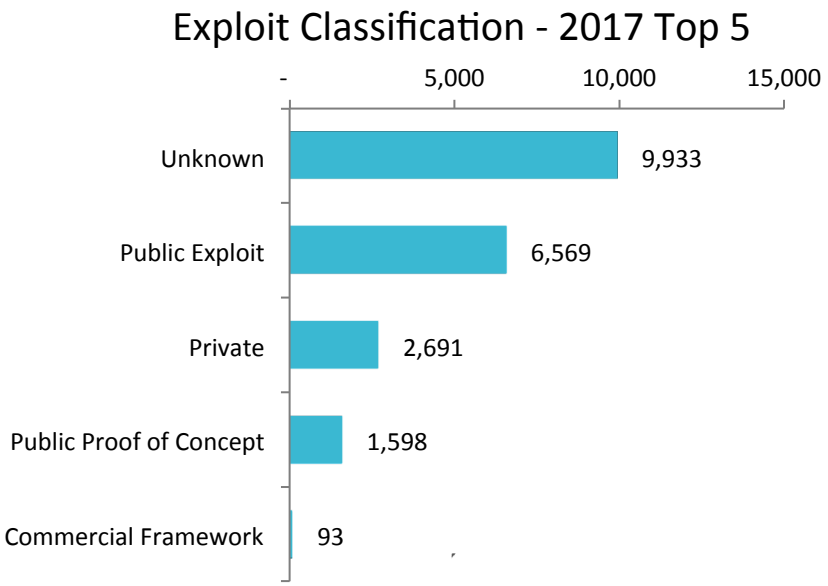
Bug bounty programs are still a hot topic in InfoSec, and still debated in many ways. It is clear that many vendors have found value in such programs, while third-party programs such as the Zero Day Initiative (ZDI) still handle an incredible number of disclosures on behalf of researchers. **While the vendor bug bounty count appears quite low, remember that a significant number of vendor bounty programs also cover services, which are out of scope for vulnerability databases.** Further, while many vendors utilize a third-party platform like HackerOne, they do not always indicate if a bounty was paid out or not. In the future, RBS hopes that vendors will be more accurate in their disclosures and flagging of such bounties.

Vulnerability Impact



The chart above, based on the classic 'CIA' triad model, where risks and vulnerabilities were broken down to those impacting confidentiality, integrity, or availability, is still useful to many organizations. **Of all the vulnerabilities aggregated in 2017, 61% affected the integrity of the products**. This ranges from various types of data manipulation such as SQL injection to the prevalent cross-site scripting to arbitrary code execution issues.

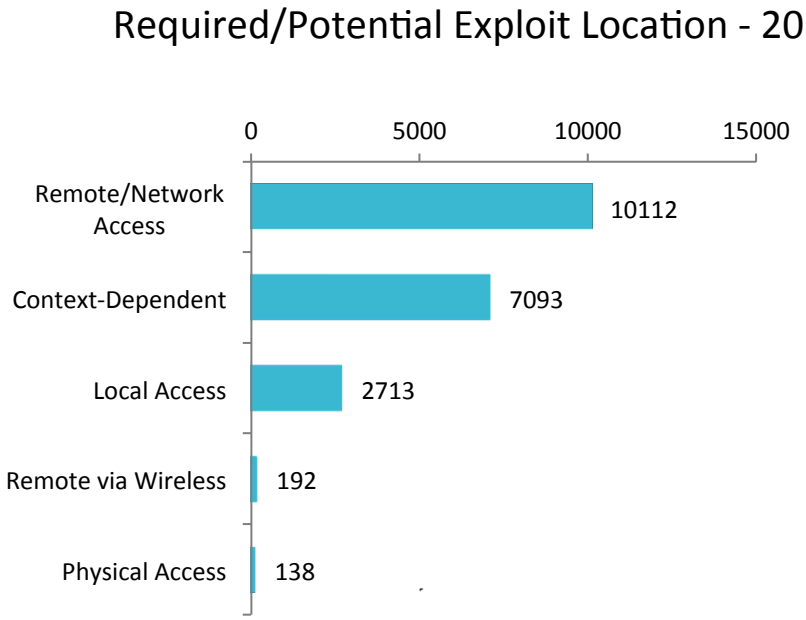
Exploit Availability



39.5% of all vulnerabilities either had exploits available or sufficient details published to generate a functioning exploit.

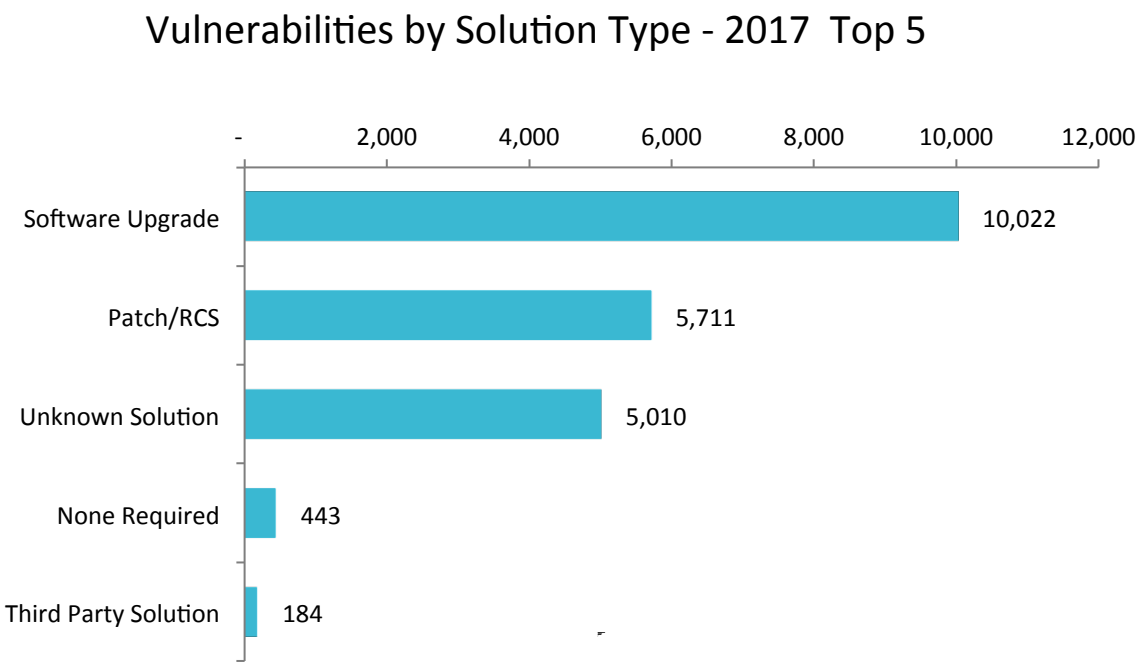
The published exploits any given year should be taken as a minimum. Over time, exploits may be written for older vulnerabilities and inserted into vulnerability scanners or published on the web. In other cases, private vulnerabilities may be released publicly.

Exploit Location



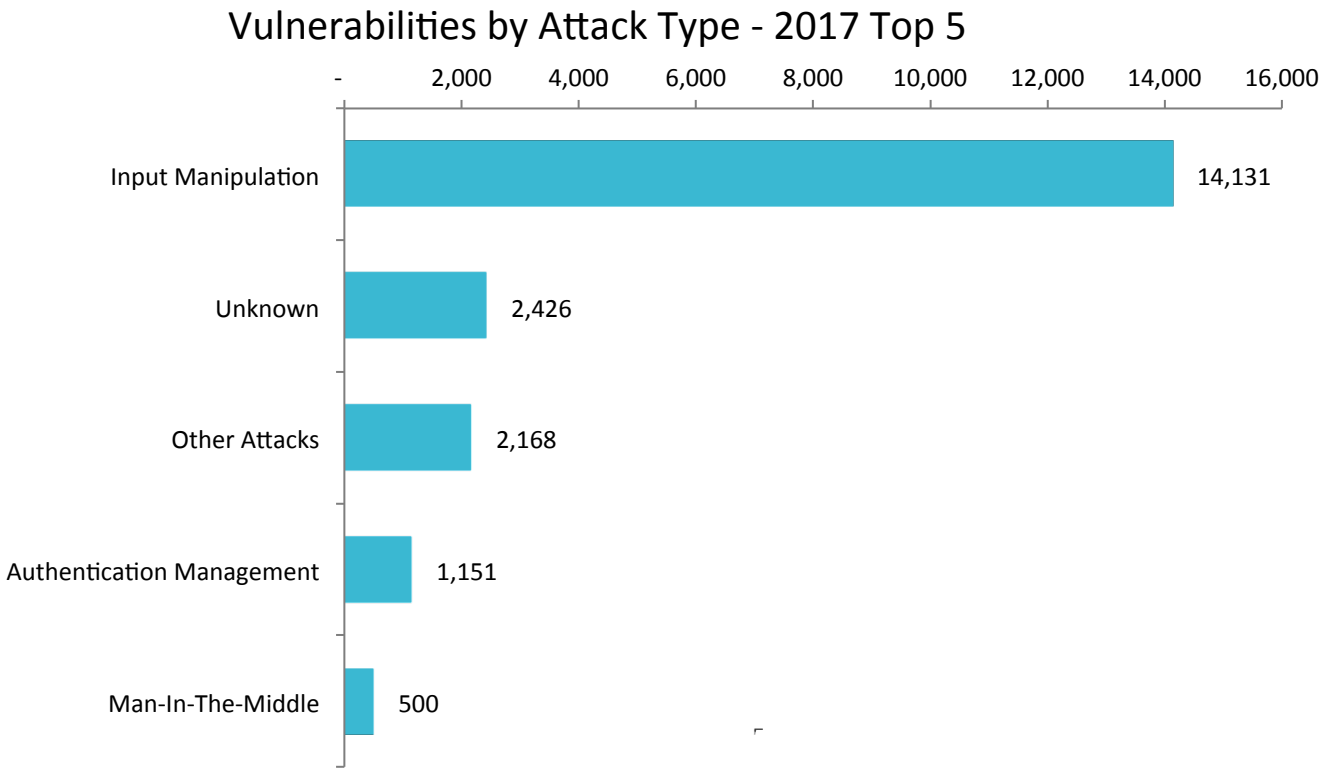
Around **half all reported vulnerabilities in 2017 have a remote attack vector** (49.9%) followed by about **a third having a "context-dependent" attack vector** (35.0%), meaning that depending on the implementation of the software, it could require local, remote, or user-assisted vectors. Overall, few of the reported vulnerabilities require some type of physical proximity to a system or device to be exploited, even if they sometimes make big headlines.

Vulnerability Solutions



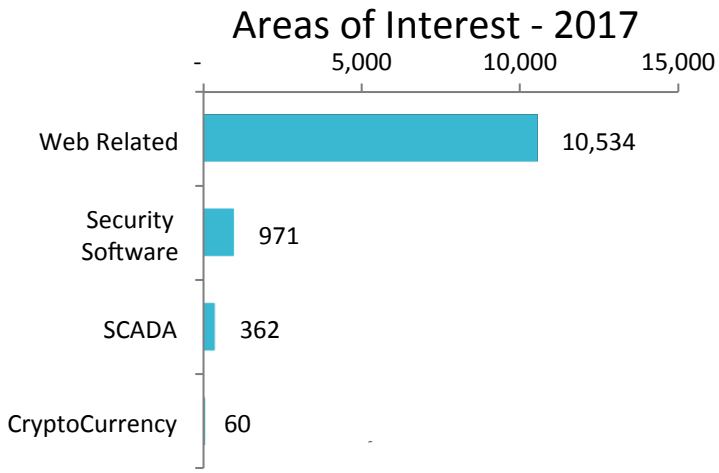
A large number of the vulnerabilities reported in 2017 have either updated versions or some form of patches available (72.8%). **However, 23.2% of the reported vulnerabilities currently have no known solution.** This underlines that while patching is very important, it cannot be solely relied on. A modern vulnerability management approach needs to focus on the root cause, which are the actual vulnerabilities, and not solely focusing on the symptoms with patch management. Organizations can make use of detailed vulnerability intelligence to understand prioritization and the ever-changing threats. Note that some patches are in the form of RCS/Git commits and may not be practical for implementation depending on the organization's policy and deployment. Further, 443 vulnerabilities that were reported in 2017 were found to have no risk due to inaccurate disclosures, therefore no solution was necessary.

Vulnerability Attack Type



Of all the vulnerabilities disclosed in 2017, 66.7% are due to insufficient or improper input validation. While a lot of vulnerabilities fall under this umbrella, including cross-site scripting, SQL injection, shell command injection, and buffer overflows, it underlines that software developers still struggle to carefully validate untrusted input. Having a mature SDL that includes secure coding practices can iron out a lot of such issues and significantly reduce the threat from attackers.

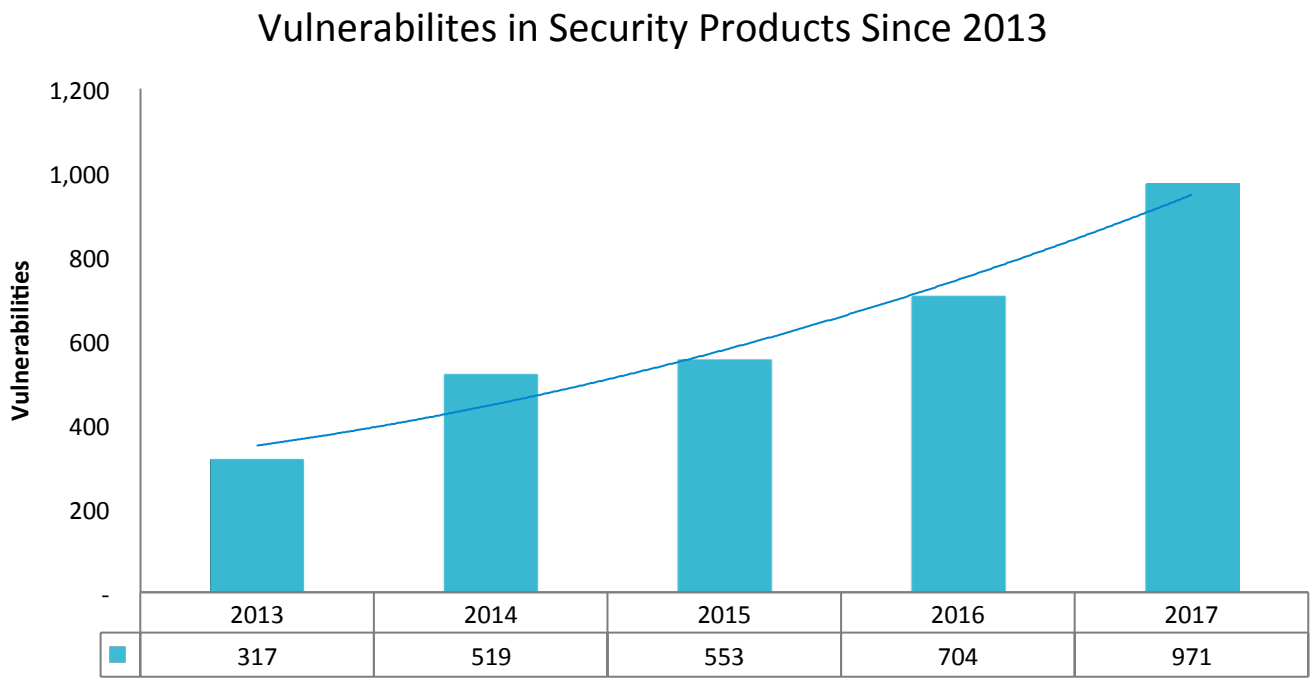
VulnDB Classifications



4.6% of the vulnerabilities reported in 2017 were discovered in security products. While such products are intended to protect organizations, they may sometimes be the weak links that allow attackers to compromise the IT infrastructure.

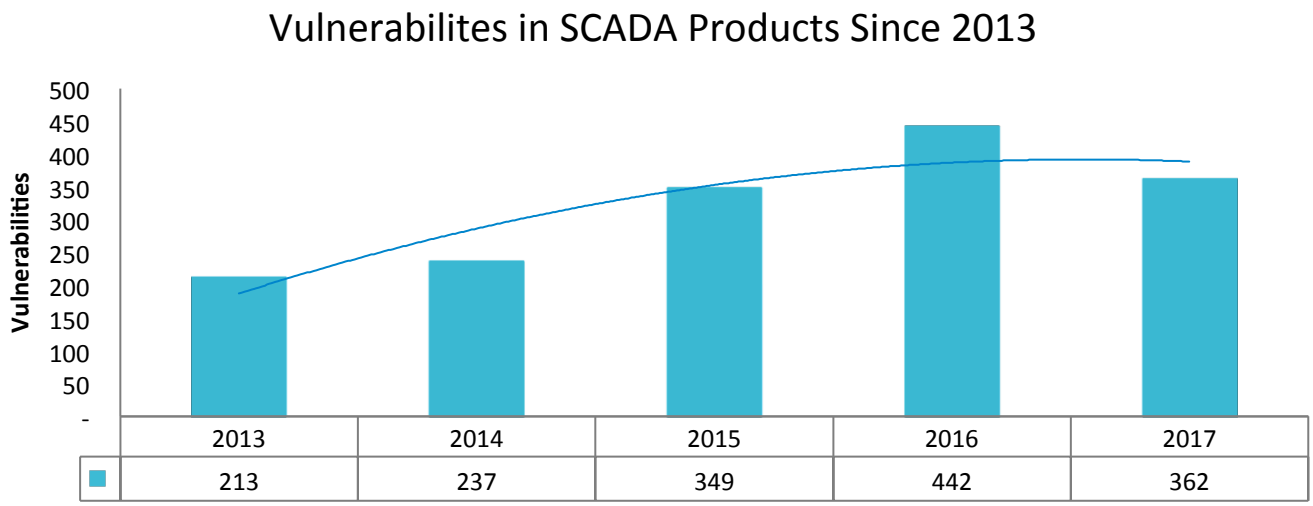
Vulnerabilities in web applications accounted for over half of the disclosures in 2017. It should be no surprise that more and more software is being made available as web applications for user convenience.

Security Software

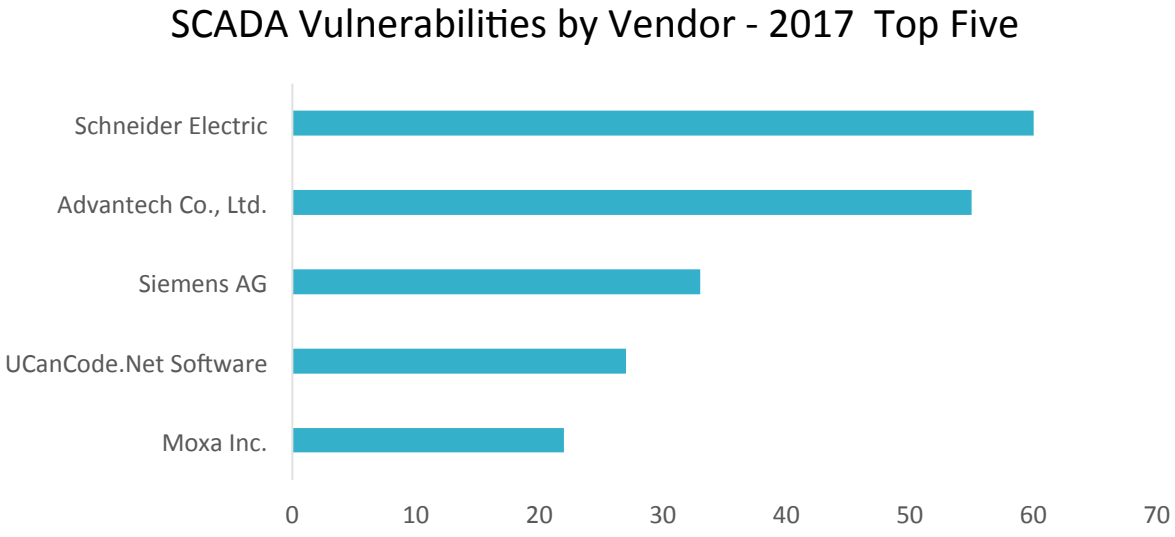


The hardware and software we purchase and deploy to protect us is becoming increasingly risky. Everything from firewalls to anti-virus to intrusion detection and prevention is being found more vulnerable. **2017 shows that researchers are taking an increased interest in testing security products, with almost 1,000 vulnerabilities being disclosed in them.** When security companies offer products that claim to "*uncover advanced threats and removes false positives*" and provide the "*ultimate protection against Internet threats*", they must be more prudent when it comes to auditing their own code. Further, these vendors should ensure that their response time to reported vulnerabilities is better than the industry average. In reality, **some security vendors had as high as a 195 day average for time to patch** and a 13 day average to respond to the vulnerability report. Given that the very same companies often have their own security research teams that find vulnerabilities in other products, they should be acutely aware of such slow times.

SCADA

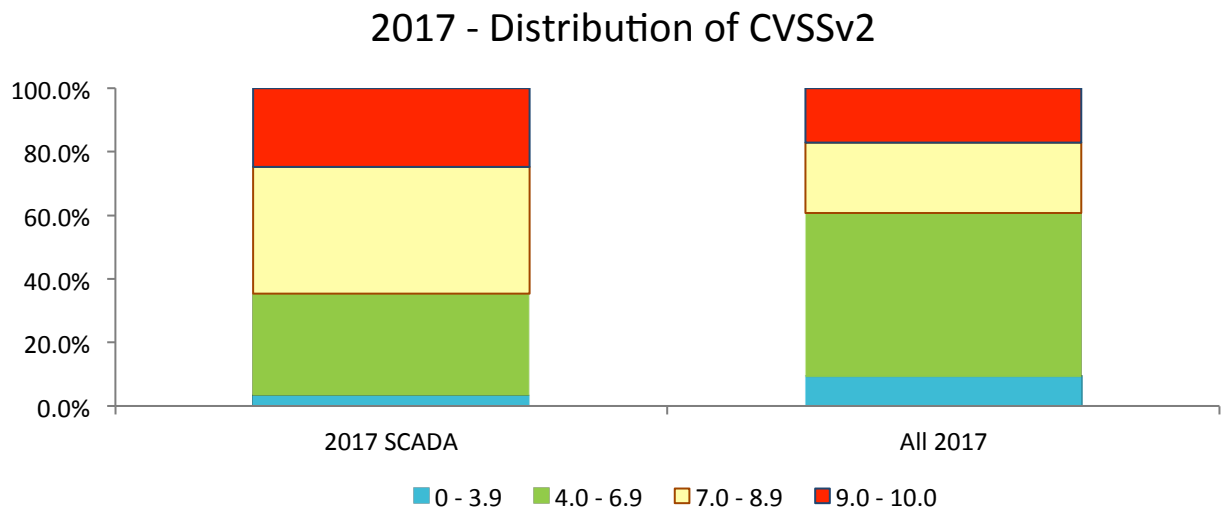


Vulnerabilities in SCADA products only accounted for 1.7% of all reported vulnerabilities in 2017, down from 2.8% in 2016. It is hard to determine if this decline in the number of vulnerabilities found in SCADA products is the result of researchers no longer focusing on SCADA products (e.g. transitioning to IoT or other software) or something else. Based on our knowledge of SCADA, it is hard to imagine it is due to SCADA security improving or vulnerabilities being more difficult to find. Despite this decrease, the potential impact for exploitation of such issues can be far greater than most organizations face.



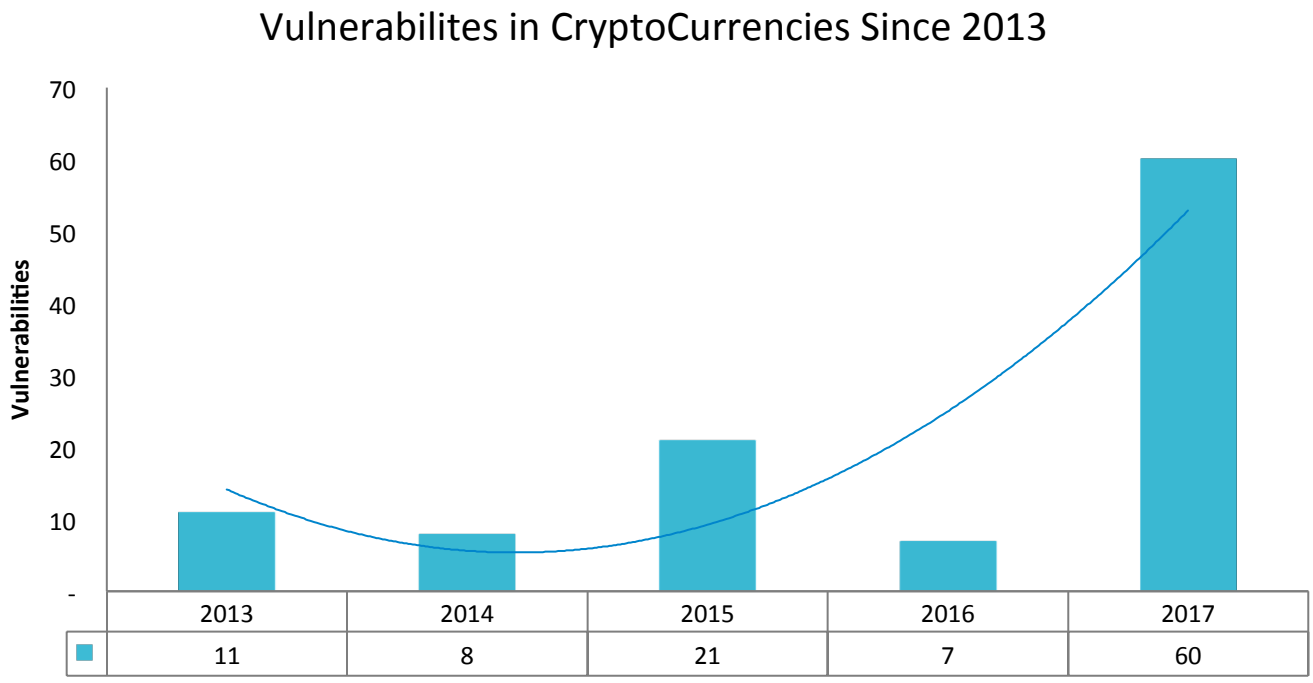
The most vulnerabilities disclosed in SCADA products in 2017 were from Schneider Electric (16.6%). This was followed by Advantech Co., Ltd. (15.9%), Siemens AG (9.1%), UCanCode.Net Software (7.5%), and Moxa Inc., (6.1%).

- **52.2% of all SCADA vulnerabilities in 2017 were remotely exploitable.**
- **61.3% of all SCADA vulnerabilities in 2017 were related to improper input validation and 10.5% were due to improper authentication management.**
- **73.5% of all reported SCADA vulnerabilities in 2017 had an impact on the integrity of the product.**



For the 2017 SCADA vulnerability disclosures, **64.6% were evaluated as High or Critical Risk** (CVSSv2 7.0 - 10.0). Given the severity of these systems and the critical infrastructure resources they control, it paints a grim picture for the potential fallout should these systems come under serious attack as we saw in the Ukraine in 2015 and 2016, and more recently, at the end of 2017 when Schneider Electric equipment was targeted in a 0-day attack that halted plant operations at an industrial facility. While there is only anecdotal evidence of human fatality as a result of a computer-based attack against SCADA systems, the threat is real.

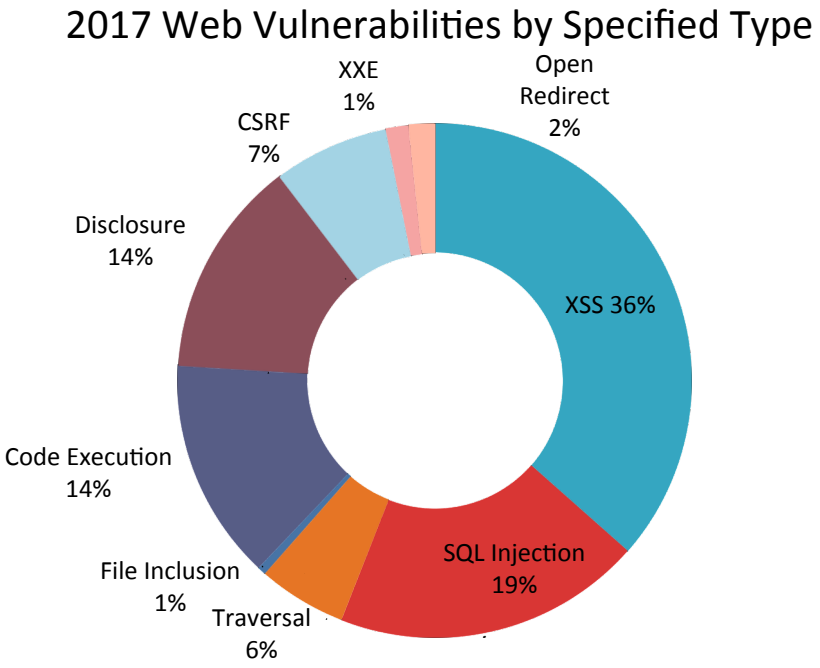
CryptoCurrency and Blockchain



With Bitcoin dominating news cycles in late 2017, the interest in CryptoCurrencies and blockchain technology is intense. Most articles seem to focus on the wild growth in Bitcoin's value, or the promise of how blockchain can seemingly solve all problems. Companies with little to no experience in the technology appear to become experts overnight.

For years, Risk Based Security has been interested in this technology from the vulnerability standpoint. By monitoring a variety of projects ranging from hobby forks of larger projects to the central Bitcoin protocols and clients, we have cataloged 121 vulnerabilities in this technology historically, half of which were disclosed in 2017 alone. Along with the media hype surrounding the prospects of becoming rich off CryptoCurrency, researchers are also taking note for different reasons. **The most interesting aspect of this, to us at least, is that blockchain technology is offering us new sub-classes of vulnerabilities**. While fundamentally they are often based on flaws in cryptography, the impact is different. Being able to manipulate remote clients to slow down their mining in order to increase your chance of discovering X, remote contract manipulation, dreaded 'double-spend' issues, and even the classic remote code execution plague many of these technologies.

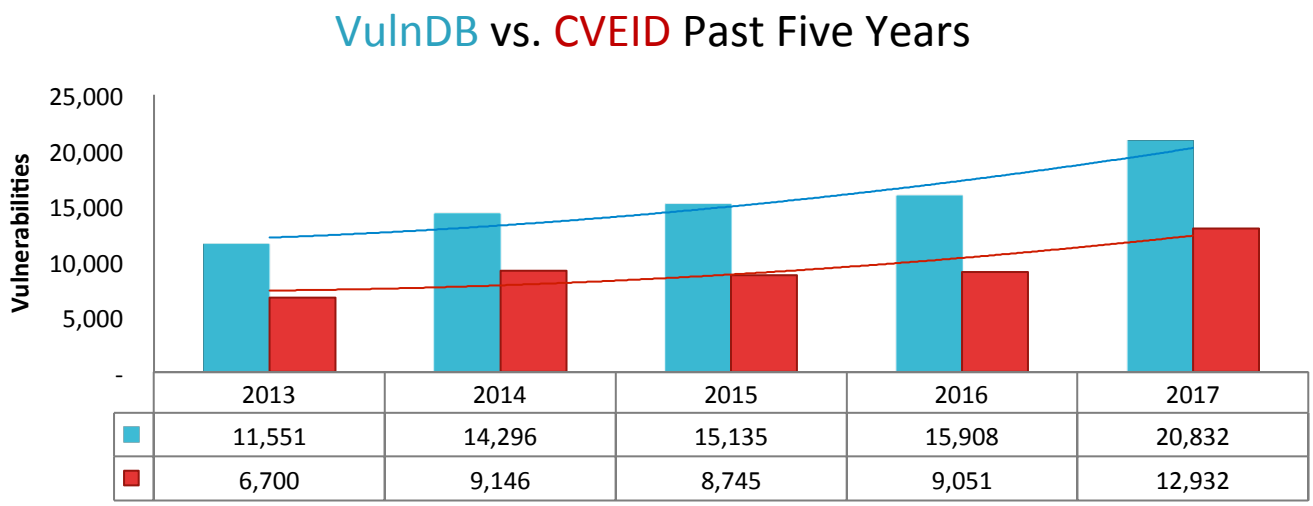
Web Vulnerabilities by Type



While basic vulnerability types have been known for many years, **web applications are still riddled with SQL injection and Cross-Site Scripting (XSS) vulnerabilities.** These account for over half of all vulnerabilities reported in web applications in 2017. Despite there being increased awareness and libraries to help sanitize input, these issues remain prevalent.

Organizations producing web-based software can utilize this type of data to better determine what testing is required for their products before shipping. Code auditing and black-box testing must be robust and look for all types of vulnerabilities, not just focus on the higher profile issues like cross-site scripting and SQL injection. While you may think that a remote information disclosure is not as big an issue, such issues certainly can be if it discloses user credentials.

DOES BETTER DATA MATTER?



	2013	2014	2015	2016	2017
	11,551	14,296	15,135	15,908	20,832
	6,700	9,146	8,745	9,051	12,932

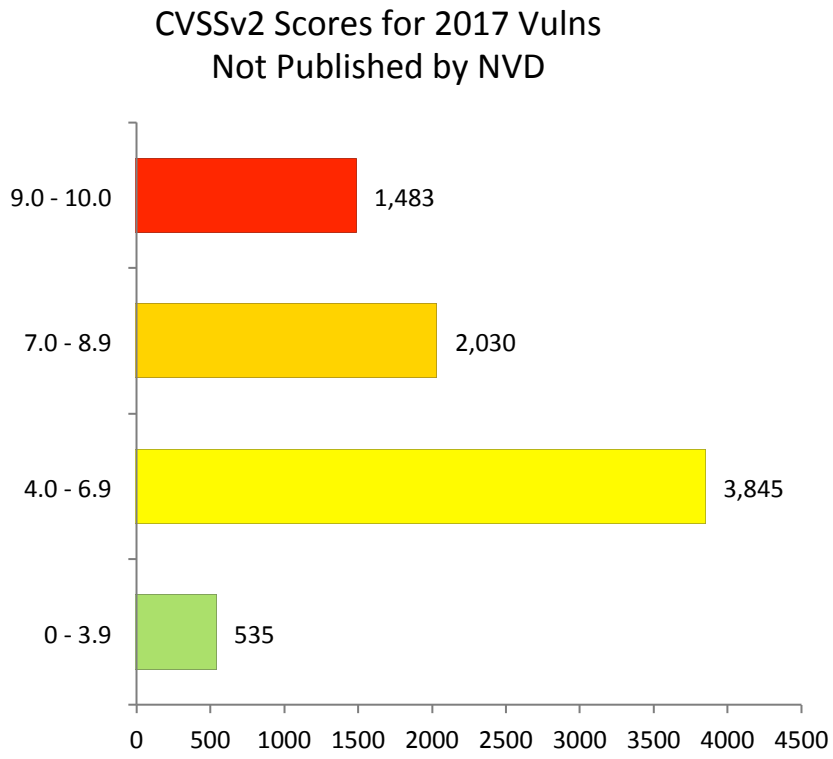
The side-by-side view of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier associated with a public disclosure for each point from 2013 to 2017, make it very clear that organizations relying on CVE/NVD or sources solely obtaining data from CVE/NVD are missing an ever increasing number of the vulnerabilities disclosed. As of January 15th, 2018 VulnDB has cataloged over 57,000 publicly disclosed vulnerabilities that you will not find in CVE/NVD. These include issues in major vendors such as Microsoft, Oracle, Apple, and Cisco, and include a variety of impacts up to and including remote code execution.

The number of vulnerabilities assigned an identifier by CVE/NVD during 2017 was also at an all-time high, mirroring the overall trend. That said, the numbers above reflect the number of CVE that are open and associated with a disclosure during that year. These numbers include a portion of the CVE in RESERVED status as well as the CVE in REJECTED status. Although missing 7,901 vulnerabilities so far in 2017 (34.0%), the number of CVE identifiers released in 2017 represent a 30.0% increase from the same reporting period in 2016. At this same time in 2016, CVE/NVD was missing 6,857 vulnerabilities reported in VulnDB or (43.2%).

By the numbers, despite CVE/NVD making efforts to address coverage issues after industry and Congressional pressure, 2017 shows that they are actually falling further behind. Along with the drop in quality of CVE entries, this firmly demonstrates that CVE/NVD is no longer "*good enough*" for your organization's vulnerability management.

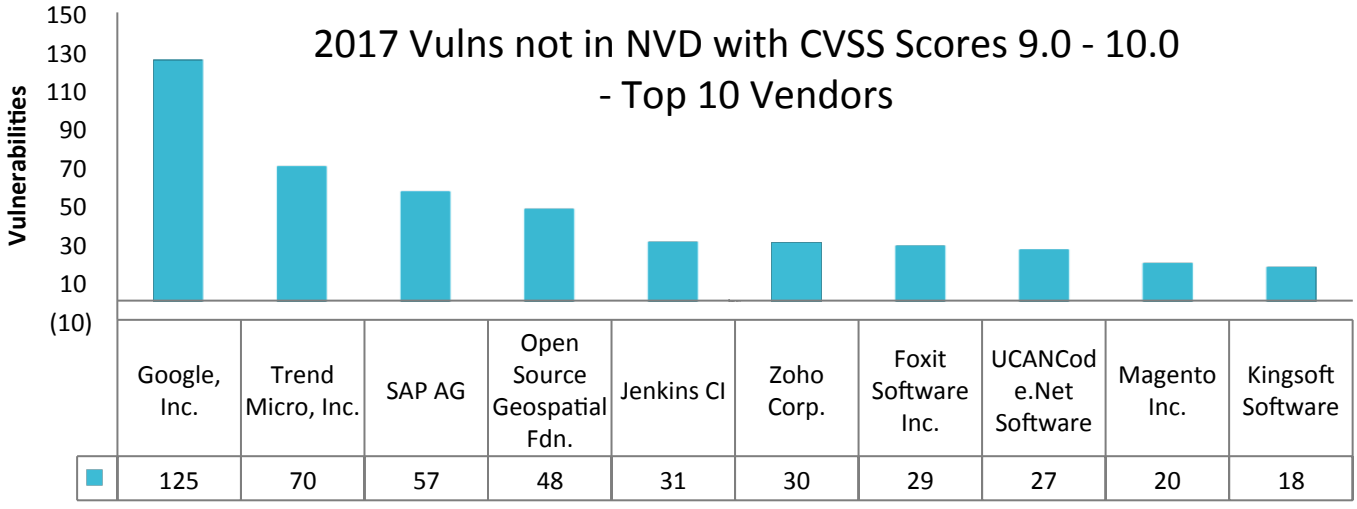
For those organizations depending on CVE/NVD compared to the same period in 2016, 2017 has averaged 1,078 vulnerabilities per month compared to 723 in 2016, a 33.0% increase. 2017 also demonstrated that MITRE and the CNAs do not follow consistent rules on assignments by year (e.g. CVE-YEAR-####) nor abstraction rules. Using the raw CVE data, it is extremely difficult to determine a given number regarding disclosures. Since some CVE identifiers represent a single vulnerability while others may represent multiple vulnerabilities, and the year identifier may not match the disclosure year, such stats can only be generated when used in conjunction with a more precise data set.

VulnDB vs. CVE/NVD Comparisons

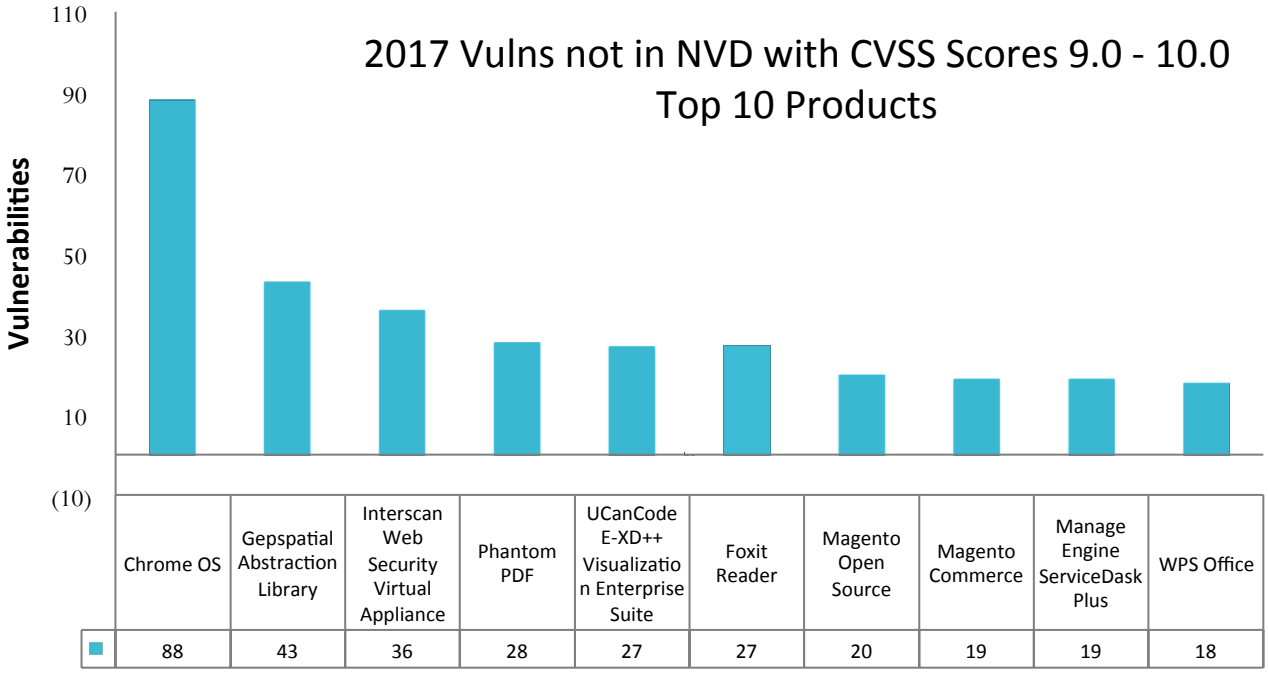


18.77% of vulnerabilities not found in CVE/NVD are scored as Critical Risk, (9.0 – 10)

A common misconception is that vulnerabilities not assigned a CVE identifier are affecting obscure products and are minor weaknesses. However, as the table and chart below plainly show, many of the "missing" vulnerabilities impact major vendors, prevalent products, and have been scored 'High' or 'Critical' severity. These vulnerabilities are of critical importance to organizations relying on CVE/NVD for data, as they cannot properly evaluate risk without the full picture.



Of the 57,000 vulnerabilities covered in VulnDB that are not in CVE/NVD, many of them are in software made by significant vendors. They span from companies such as Google and key third-party libraries that are integrated into significant projects, to mid-range companies providing software to organizations of all sizes such as Trend Micro, SAP, and Zoho.



One of the common questions we receive after someone hears that we cover over 57,000 vulnerabilities not in CVE is along the lines of "*but are they vulnerabilities in software people use?*" The answer is a resounding **yes**. The vulnerabilities cover everything from enterprise software to security software such as anti-virus, from browsers to third-party libraries that can be found in hundreds or thousands more software packages.

The Three Biggest Challenges in Vulnerability Tracking

Over the past many years, we've observed some changes to how vulnerabilities are being reported. These greatly impact how organizations need to deal with vulnerabilities reported in the products they use as well as the overall value of having access to a vulnerability intelligence solution.

More vulnerabilities are being reported than ever before

As disclosed in our previous VulnDB quarterly and annual reports, the number of vulnerabilities has been steadily climbing each year since 2011. In 2010, a bit less than 10,000 vulnerabilities were reported. This year more than 20,000 vulnerabilities were disclosed. There are various reasons for this increase in numbers including more software being created and a growing focus on vulnerability research.

Vulnerability reporting has become more decentralized

Back in early 2000, an organization interested could generally cover the majority of reported vulnerabilities by monitoring a few mailing lists and a handful of the major vendors' security pages. Where years ago the previously popular Full-Disclosure and Bugtraq mailing lists saw hundreds of reports every single month, they rarely get more than 100 posts a month these days - and sometimes only half of that.

This is a stark contrast to the sharp rise in the number of vulnerability reports. If vulnerabilities are no longer published on mailing lists, where are they then reported? The answer is: "Everywhere and anywhere." Today, at Risk Based Security we are monitoring thousands of sources ranging from the classic mailing lists and vendor security pages to social media, the deep web, researchers' own blogs, security companies' advisory pages, product bug trackers, and commits. And we're continuously adding new ones!

The quality of vulnerability reports has generally fallen

With so many vulnerabilities being reported and coming from so many different sources, it likely comes as no surprise that the quality of the average vulnerability report has dropped substantially. Poor vulnerability reports are published on a daily basis with various critical inaccuracies and omissions like affected version or references to available fixes. Other reports are outright invalid or duplicates of already known vulnerabilities. What makes matters more difficult and confusing for organizations is that some of these invalid reports and duplicates still end up with CVE identifiers assigned due to insufficient vetting.

There are many reasons for this drop in quality, but they all ultimately result in the need for a much larger and more costly effort to find and then digest published vulnerability reports.

The vulnerability impact to organizations

Obviously, the three factors above combine to have a great impact to organizations trying to stay up-to-date on the latest vulnerabilities impacting their IT infrastructure. It makes the process a lot more difficult and resource intensive. Organizations either need to ramp up the assigned resources in their vulnerability management team or accept the risk that they may not be aware of relevant and potentially serious vulnerabilities impacting their assets.

Neither of these two options are great and may ultimately come at great cost.

In the past, while not advisable, it was possible for an organization to at least cover the basics themselves. These days it is too costly and resource intensive. It is no longer a question of "*if you can do it yourself*", but "*why would you even consider doing it yourself?*"

The precious and highly paid resources it requires to gather and assess reported vulnerabilities on a daily basis is too great, when the task can be outsourced for much less than the salary of a single employee. More importantly, it frees up these resources for more important tasks to secure your organization's IT infrastructure.

The Solution

Fortunately, there is a third option that allows saving critical resources for more important tasks. Relying on a comprehensive and detailed Vulnerability Intelligence solution. We believe RBS' VulnDB solution is the answer. Gaining access to vulnerability data from a provider such as VulnDB, your employees can focus on adding more value by determining how these vulnerabilities impact your organization and addressing them.

If you are not already implementing a vulnerability intelligence solution today, you should make it a priority to contact RBS in 2018!

For a complete discussion on this topic, we recommend reading the blog "*What You Don't Know About The Vulnerability Ecosystem Can Lead To A Data Breach*" by our Chief Research Officer.

Methodology & Terms

Gathering and reporting vulnerability intelligence is not an exact science; but decades of experience helps tremendously. Discovering the new and ever-growing number of sources of vulnerability disclosure is an everyday challenge and processing that information into a usable format requires years of experience, a high-level of expertise, and 24x7 diligence. Incomplete information in the vulnerability source, constant updates and revisions, misinterpretation, and errors in reporting all contribute to a level of confusion regarding the impact, severity, and risk a vulnerability represents.

It is important that vulnerability intelligence and statistics, just as this report, be presented in a clear, responsible, and standardized manner with the appropriate definitions, disclaimers, and notes. With full disclosure in mind, VulnDB counts only distinct vulnerabilities. Meaning, if a product includes vulnerable code from third-party dependencies it is not treated as a new vulnerability unlike the reporting of some vulnerability intelligence sources, which conveniently and artificially inflates their statistics.

Further, the CVE/NVD numbers reflected in this report are the total number of unique vulnerabilities publicly disclosed in each period that have an associated CVE ID. This number is lower than the total number of assigned CVE identifiers, which includes around 16,000 RESERVED identifiers that are associated with vulnerabilities that have **no** published information since CVE began.

No matter the author, no matter the source, vulnerability intelligence and the resulting statistics must be interpreted carefully. We encourage you to reach out to your vulnerability intelligence provider and/or your network scanning service and ask about their vulnerability data sources, update timeliness, and research methodology. The security of your information assets and perhaps the longevity of your organization may depend on it.

VulnDB provides actionable intelligence about the latest in security vulnerabilities through an easy-to-use SaaS portal, RESTful APIs, and/or e-mail alerting, integrating easily into vulnerability scanners, management reporting, and ticketing system.

VulnDB is derived from a proprietary search engine and daily analysis of thousands of vulnerability sources. Unlike some vulnerability database providers, Risk Based Security is constantly searching for and adding new sources. Unlike some vulnerability databases, we believe in collecting as many vulnerabilities as possible, and allowing the user to determine which are relevant to the organization.

No Warranty

Risk Based Security, Inc. makes this report available on an "As-is" basis and offers no warranty as to its accuracy, completeness or that it includes all the latest vulnerabilities. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based security, Inc. for more detailed data loss analysis and security consulting services.

Not Just Security, the Right Security.