The Continual Rise in Vulnerabilities ...

- There were 9,690 vulnerabilities published by Risk Based Security’s VulnDB during the first six months of 2017.
- The first half of 2017 showed a 29.3% increase over the same period in 2016.
- Risk Based Security’s VulnDB published 4,092 more vulnerabilities than CVE/NVD in the first six months.
- CVSSv2 scores above 9.0 accounted for 21.1% of all published 2017 vulnerabilities.
- 20.0% of the vulnerabilities not published by NVD/CVE have a CVSS score between 9.0 and 10.
- Coordinated disclosure accounted for ~41% of 2017 vulnerabilities.
- Major vendors such as Microsoft, Oracle, and Apple account for 30.5% of 2017 vulnerabilities.
- Web-related vulnerabilities accounted for 53.2% of 2017 vulnerabilities.
- 33.6% of 2017 vulnerabilities have public exploits.
- 74.8% of 2017 vulnerabilities have a documented solution.
- 48.6% of 2017 vulnerabilities can be exploited remotely.
- At least 5.9% of 2017 vulnerabilities were coordinated through bug bounty programs.
- 1.8% of 2017 vulnerabilities were classified as SCADA vulnerabilities.
- 35.0% of web-related 2017 vulnerabilities are Cross-Site Scripting (XXS).
Introduction to the VulnDB QuickView Report

Gathering and reporting vulnerability intelligence is not an exact science; but years of experience pays-off. Discovering the new and ever-growing number of sources of vulnerability disclosure is a daily challenge and processing that information can be even more difficult to interpret correctly. Incomplete information, constant updates and revisions, misinterpretation, and errors in reporting, can all contribute to a level of confusion regarding the impact, severity, and risk a vulnerability represents.

It is important that vulnerability statistics 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 published in each period that have an associated CVE ID. This number is lower than the total number of assigned CVE identifiers, which includes almost 10,000 RESERVED IDs that are associated with vulnerabilities that have no public information.

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 depends on it.

What does this report cover?

This report covers the vulnerabilities captured by Risk Based Security during the first six months of 2017. The information collected is displayed in a series of charts depicting various groupings, classifications, and comparisons of the data from January 1st through June 30th of 2017.

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

We hope you find the report useful!
Mid-Year 2017 Compared to the Past Four Years

The number of vulnerabilities disclosed during the first six months of 2017 was at an all-time high. Even the 1,000+ increase from 2014 to 2015 has been surpassed by the number of disclosed vulnerabilities at the mid-point of 2017, a (29.3%) jump from 2016. If this continues, 2017 is on the path to become a record-breaking year in the number of vulnerabilities disclosed!
Mid-Year 2017 by Month

Compared to the same months in 2016, June 2017 (+2%) was a relatively standard month of vulnerability disclosures, both March (+63%) and April (+56%) spiked considerably in the number of vulnerabilities disclosed. While the small increase in June compared to 2016 may indicate disclosures tapering off, it is crucial to remember that the VulnDB research team will continue adding vulnerabilities as they are disclosed from prior months throughout the year. We expect the June total to continue to grow.
Mid-Year Comparisons

**VulnDB vs. CVE First Six Month's Vulnerabilities**

The side-by-side views of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier assigned for each Mid-Year point from 2013 to 2017, make it very clear that organizations relying on CVE or sources solely obtaining data from CVE are missing almost half of all the vulnerabilities disclosed and sometimes more.

**VulnDB vs. CVE By Month in 2017**
While the number of vulnerabilities change each month, CVSSv2 scores have been relatively consistent with about half of the vulnerabilities scoring between 6.0 and 10.
A common misconception is that vulnerabilities not assigned a CVE identifier are affecting obscure products and are minor weaknesses. However, many of the vulnerabilities not only affect prevalent products, but have been scored ‘High’ or ‘Critical’ severity.

Products from major vendors account for 30.5% of the vulnerabilities reported in Q1 2017. The average CVSSv2 scores for the vulnerabilities for each vendor is in the ‘Medium’ range. The average CVSSv2 score for vulnerabilities in Adobe products was ‘High’.
Mid-Year 2017 Highlights

Note: It is important to remember bug bounty programs may be big in the news headlines, but are statistically rare for vendors. Many bounty programs are for services, not software, and there is a near 50% re-discovery rate for vulnerabilities in the popular HackerOne bounty platform for both software and services.

41.2% of 2017 vulnerabilities were coordinated with the Vendor; Just 5.9% were the result of vendor or third-party bug bounties.

Mid-Year 2017 Vulnerabilities by Impact Type

Of all the vulnerabilities reported in 2017, 63% affected the integrity of the products. This ranges from various types of data manipulation and cross-site scripting issues to SQL injection and code execution.
Almost half all reported vulnerabilities in 2017 have a remote attack vector (48.6%) followed by about a third having a user-assisted attack vector (33.1%). Overall, few of the reported vulnerabilities require some type of physical proximity to a system or device to be exploited.

Of all the vulnerabilities reported in 2017, 41.1% either had exploits available or sufficient details published to generate a functioning exploit.
A large number of the vulnerabilities reported in 2017 have either updated versions or patches available. However, 25.2% 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 only the symptoms with patch management. Organizations can make use of detailed vulnerability intelligence to understand prioritization and the ever-changing threats.
Of all the vulnerabilities disclosed in 2017, 66.6% 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 vendors 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.

5.3% 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 SCADA products only accounted for 1.8% of all reported vulnerabilities in 2017. 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.

The most vulnerabilities disclosed in SCADA products in 2017 were from Schneider Electric (31.8%). This was followed by UcanCode.NET Software (15.0%), Siemens AG (8.9%), Moxa Inc. (8.4%), and Honeywell International (2.8%) coming in 5th place.

- 66.1% of all SCADA vulnerabilities in 2017 were remotely exploitable.
- 52.7% of all SCADA vulnerabilities in 2017 were related to improper input validation and 15.0% were due to improper authentication management.
- 13.3% of all reported SCADA vulnerabilities in 2017 had an impact on the availability of the product, which is especially critical given the resources they manage.
For the 2017 SCADA vulnerability disclosures, around 20% were evaluated as High Risk or Critical (CVSSv2 9.0 - 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.

While basic vulnerability types that have been known for many years, web applications are still riddled with SQL injection and XSS (Cross-Site Scripting) vulnerabilities. These account for over half of all vulnerabilities reported in web applications in 2017.
A Word about CVSSv2 vs. CVSSv3

CVSSv3 was officially released June 2015, but industry adoption of CVSSv3 over CVSSv2 has been slow. Currently, we at Risk Based Security have not fully switched from CVSSv2 to CVSSv3, but are in the process of doing so. We first wanted to better understand the improvements and limitations of CVSSv3 and also observe its adoption rate. Many organizations are unsure by some of the changes or do not fully understand them. This even includes organizations, who have already adopted CVSSv3.

As part of our VulnDB offering, we have scored tens of thousands of vulnerabilities with CVSSv2 and were looking forward to an improved standard. While some improvements have been made, CVSSv3, unfortunately, also introduced new concerns and did not completely address some of the problems with CVSSv2. Since 2015, this became evident as vendors who struggled to score properly under CVSSv2 standards continued to score incorrectly under CVSSv3.

As part of our analysis into CVSSv3, we decided in Q1 2017 to create a very thorough and detailed blog post series about CVSSv3. This should, hopefully, assist organizations in better understanding the advantages and limitations of CVSSv3 and determine if they feel if CVSSv3 provides sufficient value to justify a switch from CVSSv2.
Methodology & Terms
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.

VulnDB counts only distinct vulnerabilities. Products sharing the same vulnerable codebase are considered as only one unique vulnerability; not counted as one vulnerability per affected product like some vulnerability databases do to inflate their statistics. To be clear, a vulnerability in a third-party library such as OpenSSL is one vulnerability. The number of products using and integrating that code are not included in the VulnDB counts. [https://vulndb.cyberriskanalytics.com/](https://vulndb.cyberriskanalytics.com/)

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.