Unrelenting Rise in Vulnerabilities …

- There were 4,837 vulnerabilities published by Risk Based Security’s VulnDB during the first three months of 2017.
- First quarter 2017 showed a 29.2% increase over the same period in 2016.
- Risk Based Security’s VulnDB published 2,274 more vulnerabilities than CVE/NVD in the first quarter.
- CVSSv2 scores above 9.0 accounted for 17.5% of all published Q1 2017 vulnerabilities.
- 15.7% of the vulnerabilities not published by NVD/CVE have a CVSS score between 9.0 and 10.
- Coordinated disclosure accounted for 41.6% of Q1 2017 vulnerabilities.
- Major vendors account for 31.1% of Q1 2017 vulnerabilities.
- Web-related vulnerabilities accounted for 58.6% of Q1 2017 vulnerabilities.
- 35.1% of Q1 2017 vulnerabilities have public exploits.
- 72.4% of Q1 2017 vulnerabilities have a documented solution.
- 50.4% of Q1 2017 vulnerabilities can be exploited remotely.
- 7.0% of Q1 2017 vulnerabilities were coordinated through bug bounty programs.
- 1.3% of Q1 2017 vulnerabilities were classified as SCADA vulnerabilities.
- 30.0% of web-related Q1 2017 vulnerabilities are SQL injection.
Introduction to the VulnDB QuickView Report

Gathering and reporting vulnerability intelligence is not an exact science. Discovering the new and ever-growing number of sources is a daily challenge and 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.

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 many RESERVED IDs that are not associated with any published vulnerabilities.

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 quarter of 2017. The information collected is displayed in a series of charts depicting various groupings, classifications and comparisons of the data from the first quarter.

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.
The number of vulnerabilities disclosed in Q1 2017 was at an all-time high. While no significant increase occurred from 2014 to 2016, the number of disclosed vulnerabilities jumped (29.2%) in Q1 2017. If this continues, 2017 is in the path to become a record-breaking year in the number of vulnerabilities disclosed!
While February 2017 (+11.0%) was a relatively standard month of vulnerability disclosures, both January (+24.6%) and March (+53.6%) spiked in the number of vulnerabilities disclosed compared to the same months in 2016.
First Quarter Comparisons

VulnDB vs. CVEID First Quarter Vulnerabilities

<table>
<thead>
<tr>
<th>Year</th>
<th>VulnDB</th>
<th>CVEID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>2,772</td>
<td>1,603</td>
</tr>
<tr>
<td>2014</td>
<td>3,326</td>
<td>1,860</td>
</tr>
<tr>
<td>2015</td>
<td>3,653</td>
<td>2,329</td>
</tr>
<tr>
<td>2016</td>
<td>3,744</td>
<td>2,002</td>
</tr>
<tr>
<td>2017</td>
<td>4,837</td>
<td>2,563</td>
</tr>
</tbody>
</table>

VulnDB vs. CVEID First Quarter 2017

<table>
<thead>
<tr>
<th>Month</th>
<th>VulnDB</th>
<th>CVEID</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAN</td>
<td>1,703</td>
<td>980</td>
</tr>
<tr>
<td>FEB</td>
<td>1,352</td>
<td>630</td>
</tr>
<tr>
<td>MAR</td>
<td>1,782</td>
<td>953</td>
</tr>
</tbody>
</table>

Side-by-side views of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier assigned for each Q1 from 2013 to 2017. The graphs make it very clear that organizations relying on CVE or sources solely obtaining data from CVE are missing about half of all the vulnerabilities disclosed and sometimes more.
First Quarter CVSS Comparisons

While the number of vulnerabilities change each month, CVSSv2 scores have been relatively consistent with about half of the vulnerabilities scoring as ‘High’ (9.0-10) or ‘Critical’ 6.0- 8.99).
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 do affect prevalent products, but have a ‘High’ or ‘Critical’ severity.

Products from major vendors account for 31.1% 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’.
First Quarter 2017 Highlights

Of all the vulnerabilities reported in Q1 2017, 68% 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.

41.6% of Q1 vulnerabilities were coordinated with the Vendor; Just 7.0% were the result of Bug Bounties.

Q1 2017 Vulnerabilities by Impact Type

- Confidentiality: 18%
- Integrity: 68%
- Availability: 10%
- Unknown: 4%

Of all the vulnerabilities reported in Q1 2017, 68% 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.
About half of all reported vulnerabilities in Q1 2017 have a remote attack vector followed by about 1/3 having a user-assisted attack vector. Overall, few of the reported vulnerabilities require local access to a system or device.

Of all the vulnerabilities reported in Q1 2017, 35.1% either had public exploits available or sufficient details published to trivially exploit.
A large number of the vulnerabilities reported in Q1 2017 have either updated versions or patches available. However, 28.9% 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 Q1 2017, 68.1% 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 can iron out a lot of such issues and significantly reduce the threat from attackers.

6.7% of the vulnerabilities reported in Q1 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 1.3% of all reported vulnerabilities in Q1 2017. However, this decline in the number of vulnerabilities found in SCADA products seems to reflect the fact that researchers are no longer focusing on SCADA products rather than a significant improvement in SCADA product security.

SCADA Vulnerabilities by Vendor Q1 2017 - Top Five

The most vulnerabilities disclosed in SCADA products in Q1 2017 were from Schneider Electric (23.4%). This was followed by Siemens (15.6%), Moxa (10.9%), Honeywell (7.8%), with Advantech (4.7%) and Carlo Gavazzi Automation (4.7%) sharing 5th place.

- 73.4% of all SCADA vulnerabilities in Q1 2017 were remotely exploitable.
- 43.5% of all SCADA vulnerabilities in Q1 2017 were related to improper input validation and 22.6% were due to improper authentication management.
- 65.2% of all reported SCADA vulnerabilities in Q1 2017 had an impact on the data integrity of the product, ranging from data manipulation to code execution.
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 2/3 of all vulnerabilities reported in web applications in Q1 2017.

A Word about CVSSv2 vs. CVSSv3

CVSSv3 was officially released June 2015, but adoption of CVSSv3 over CVSSv2 has been slow. Currently, we at Risk Based Security have not 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 improvements have been made, CVSSv3, unfortunately, also introduced new concerns and did not completely address some of the problems with CVSSv2.

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.

We strongly recommend anyone using or planning on using CVSSv3 to read the blog series, which is available at our website: https://www.riskbasedsecurity.com/2017/01/cvssv3-newer-is-better-right/
Methodology & Terms

VulnDB provides actionable intelligence about the latest in security vulnerabilities through an easy-to-use SaaS portal, database export, or 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.

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.