The Continuing Rise in Vulnerabilities:

- There were 5,375 vulnerabilities published by Risk Based Security’s VulnDB team during the first three months of 2018.
- First quarter 2018 showed just a 1.8% increase over the same period in 2017.
- Risk Based Security’s VulnDB published 1,790 more vulnerabilities than CVE/NVD in the first quarter alone.
- CVSSv2 scores of 9.0+ accounted for 18.0% of all published Q1 2018 vulnerabilities.
- 19.7% of the vulnerabilities not published by NVD/CVE have a CVSS score between 9.0 and 10.
- Coordinated disclosure accounted for 47.2% of Q1 2018 vulnerabilities. 6.2% of coordinated disclosures were through bug bounty programs.
- Eight major vendors accounted for 22.9% of Q1 2018 vulnerabilities.
- Web-related vulnerabilities accounted for 47.5% of Q1 2018 vulnerabilities.
- 32.7% of Q1 2018 vulnerabilities have public exploits.
- 74.3% of Q1 2018 vulnerabilities have a documented solution.
- 49.1% of Q1 2018 vulnerabilities can be exploited remotely.
- 1.5% of Q1 2018 vulnerabilities were classified as SCADA vulnerabilities.
- 1.80% of Q1 2018 vulnerabilities were classified as impacting security software.
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 2018. 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 2018 was at an all-time high. While no significant increase occurred from 2014 to 2016, the number of disclosed vulnerabilities jumped 27.92% in Q1 2017, while only increasing 1.8% in Q1 2018. Despite this small increase, RBS fully expects 2018 to continue the trend and be another record-breaking year for disclosed vulnerabilities.
The Q1 trends in 2018, as compared to 2017, are interesting. January saw a small increase (1.17%) over the previous year, while February saw a considerable jump (22.32%). March came in at a significant decrease at the time of this report (-21.34%). However, it is typical that throughout the year vulnerabilities will be added for prior months. As such, we expect March to have a significant increase when we publish the 2018 mid-year and end-of-year reports.
First Quarter 2018 Comparisons

**VulnDB vs. CVEID Q1 Past Five Years**

- 2014: 3,342
- 2015: 3,684
- 2016: 3,808
- 2017: 5,278
- 2018: 5,375

**VulnDB vs. CVEID Q1 By Month**

- JAN: 1,799
- FEB: 1,922
- MAR: 1,654

Side-by-side views of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier assigned for the first quarter from 2014 to 2018. The graphs make it very clear that organizations relying on CVE or sources solely obtaining data from CVE are missing a significant number of disclosed vulnerabilities. In today’s hostile computing environment, with non-stop attacks from around the world, organizations using sub-par vulnerability intelligence are taking on significant risk.
While the number of vulnerabilities change each month, CVSSv2 scores have shifted down in March, with just 33.5% scored as ‘High’ (7.0-8.99) or ‘Critical’ (9.0-10.0). The first quarter of 2018 showed a shift to more disclosures falling in the 'Medium' (4.0 - 6.9) range.

19.7% of vulnerabilities not found in CVE/NVD are scored 9.0 - 10
First Quarter 2018 Highlights

Vulnerability Disclosure Path - 2018

- Coordinated Disclosure: 2,537 vulnerabilities
- Uncoordinated Disclosure: 1,044 vulnerabilities
- Bug Bounty (Non Vendor): 268 vulnerabilities
- Bug Bounty (Vendor): 65 vulnerabilities

47.2% of 2018 Q1 vulnerabilities were coordinated with the Vendor, an increase from 2017 Q1. Just 6.1% were the result of Bug Bounties.

Note that bug bounties are a subset of the 'Coordinated Disclosures' total.

2018 Q1 Vulns by Impact Type

- Confidentiality: 18%
- Unknown: 8%
- Integrity: 56%
- Availability: 18%

Of all the vulnerabilities reported in Q1 2018, 56% 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 2018 have a remote attack vector followed by almost a third having a user-assisted (Context-Dependent) attack vector. Overall, few of the reported vulnerabilities require local access to a system or device. Vulnerabilities that require access via Wireless, a subset of Remote, only accounted for 4%.
Of all the vulnerabilities reported in Q1 2018, 40.8% either had public exploits available or sufficient details published to exploit the vulnerability (a working proof-of-concept or PoC).
A large number of the vulnerabilities reported in Q1 2018 have either updated versions or patches available. However, 24.1% 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 be more than just patch management, it needs to make use of detailed vulnerability intelligence to understand and prioritize mitigation actions to address the ever-changing threats. Detailed information on the threats your organization faces can be used to better implement broader mitigation strategies including compensating security controls.
Of all the vulnerabilities disclosed in Q1 2018, 67.0% 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 Software Development Lifecycle (SDL) can help iron out a lot of such issues and significantly reduce the threat from attackers.
CryptoCurrency and Blockchain: The Latest Rage

Blockchain technology, the foundation of CryptoCurrency such as Bitcoin, Ethereum, and countless others is starting to dominate the news. With the wild ride of Bitcoin prices, where one coin was worth around $19,000 in December, 2017 and a drastic fall in February, 2018 to around $6,900, the financial industry is abuzz with the possibilities. Many would-be entrepreneurs are looking to get involved, while few organizations are monitoring the vulnerabilities in this technology. Risk Based Security has been studying the security aspects for many years and has been collecting the vulnerabilities that range from annoying remote denial of service conditions, to vulnerabilities that allow a single person to mint as many coins as they like, that could lead to serious destabilization of the currency. In the coming months, we will be publishing an extensive blog on the topic of vulnerabilities in the CryptoCurrency market as we continue to aggregate blockchain-based vulnerabilities.

Blockchain Technology Vulnerabilities
Case Study: SCADA Vulnerabilities
Supervisory Control And Data Acquisition (SCADA) systems are generally considered the systems that run public infrastructure, ranging from power plants and electric grids to dams and spillways. Vulnerabilities in such systems can have catastrophic consequences as we saw in 2015 when Ukraine’s power grid was attacked and portions of the country lost power due to computer intrusion. It is believed to be the first attack against SCADA systems that resulted in wide-scale power outages. Ukraine was attacked again in 2017 using modified ransomware, that affected a wide variety of systems including radiation monitors at Ukraine’s Chernobyl Nuclear Power Plant. These devastating attacks, according to some experts, are a hint of what may come if SCADA systems are not secured in short order.

SCADA Vulnerabilities

2017 saw a significant drop in SCADA disclosures, which led us to speculate in our 2017 End of Year report:

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.

This year, the first quarter shows an increase in SCADA disclosures, enough to suggest that this may be a new record year.
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/

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.