The Continuing Rise in Vulnerabilities:

- There were 10,644 vulnerabilities published by Risk Based Security’s VulnDB team during the first half of 2018.
- First half of 2018 showed less than a 1% increase over the same period in 2017.
- Risk Based Security’s VulnDB published 3,279 more vulnerabilities than CVE/NVD in the first half of 2018.
- CVSSv2 scores of 9.0+ accounted for 16.6% of all published mid-year 2018 vulnerabilities.
- 23.1% of the vulnerabilities not published by NVD/CVE have a CVSS score between 9.0 and 10.
- Coordinated disclosure accounted for 48.2% of mid-year 2018 vulnerabilities. 13.1% of coordinated disclosures were through bug bounty programs.
- Five major vendors accounted for 16.4% of 2018 vulnerabilities so far.
- Web-related vulnerabilities accounted for 46.3% of 2018 vulnerabilities.
- 32.1% of 2018 vulnerabilities have public exploits.
- 73.1% of 2018 vulnerabilities have a documented solution.
- 50% of 2018 vulnerabilities can be exploited remotely.
- 3.1% of 2018 vulnerabilities were classified as SCADA vulnerabilities.
- 4% of 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. In many cases, RBS will have a vulnerability with an associated CVE ID that is in RESERVED status, which inflates CVE's numbers in this report.

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 half of 2018. The information collected is displayed in a series of charts depicting various groupings, classifications, and comparisons of the data collected so far in 2018.

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 the first half of 2018 was at an all-time high, but just marginally more than last year. While no significant increase occurred from 2014 to 2016, the number of disclosed vulnerabilities jumped 28.1% in the first half of 2017, while only increasing 0.1% in the first half of 2018. Despite this small increase, RBS fully expects 2018 to continue the trend and be another record-breaking year for disclosed vulnerabilities.
The trends in the first half of 2018, as compared to 2017, are interesting. January saw a small increase (3.62%) over the previous year, while February saw a considerable jump (24.32%). March came in at a significant decrease at the time of this report (-15.30%). However, it is typical that throughout the year vulnerabilities will be added for prior months. As such, we expect June to have a significant increase when we publish the 3Q2018 report.
First Half-year Comparisons

Above are side-by-side views of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier assigned and related to a public disclosure for the first half of each year between 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 needlessly.

If an organization is unaware of all the vulnerabilities, how can they be sure to act on the vulnerabilities posing the greatest risk to their assets? Furthermore, many CVEs are published significantly later than the vulnerabilities in VulnDB.
Looking at the CVSSv2 trends for disclosures in the first half of 2018, February appears to be a small outlier. In addition to having the least amount of 'Low' severity vulnerabilities (7.6% between 0.0 - 3.9), it also has the highest number of 'Critical' vulnerabilities (19.6% between 9.0 - 10.0). The spike in February can largely be attributed to over 280 critical vulnerabilities patched in Samsung mobile devices. As usual, a majority of disclosures continue to fall in the 'Medium' (4.0 - 6.9) range.

CVSSv2 for 2018 Q1/Q2 Vulns
Not Published by NVD

There are 1,524 vulnerabilities, (High and Severe Risk), that have not been cataloged by NVD. Can you afford not to know what they are?
First Quarter 2018 Highlights

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

So far, 48.5% of 2018 vulnerabilities were coordinated with the vendor, a small increase from Q1. Just 7.1% were the result of Bug Bounties.

Of all the vulnerabilities reported in 2018, 58% 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 2018 have a remote attack vector followed by almost a third having a user-assisted (Context-Dependent) attack vector. Overall, a little over 10% 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 1.1%. About 6.6% of vulnerabilities were related to mobile devices, regardless of exploit location.
Of all the vulnerabilities reported in 2018, 41.1% either had public exploits available or sufficient details published to exploit the vulnerability (a working proof-of-concept a.k.a. PoC). Over 13% of vulnerabilities had a working exploit that was not published by the researchers.
A large number of the vulnerabilities reported in 2018 have either updated versions or patches available. However, 25.6% 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 2018, 67.2% 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 from users. Having a mature Software Development Lifecycle (SDL) and some form of auditing can help iron out a lot of such issues and significantly reduce the threat from attackers.
Vulnerability Timeline Exposure Metrics (VTEM)

Recently, Tenable Network Security posted a blog titled "Quantifying the Attacker’s First-Mover Advantage". From the blog:

Tenable Research has just released a report on the difference in time between when an exploit is publicly available for a given vulnerability and the first time that a vulnerability is assessed.

For this study, we analyzed the 50 most prevalent critical and high-severity vulnerabilities from just under 200,000 vulnerability assessment scans over a three-month period in late 2017 to anchor the analysis to the real world. We used these vulnerabilities to derive the “time to exploit availability” and “time to assess” to calculate the median delta.

This metric, which RBS refers to as "time to exploit", is based on the time between the vendor solution date and the exploit publish date. RBS also tracks "total time to exploit", which measures the time between vulnerability discovery and exploit publication. These are two of six metrics RBS tracks in what we call the Vulnerability Timeline Exposure Metrics or VTEM.

While the Tenable report is interesting reading, (looking at just 50 vulnerabilities), having the full set of metrics from VTEM for every vulnerability, (when the dates are published), is truly powerful. VTEM can be used to generate a more comprehensive view of a piece of software or vendor, giving users a quick idea of the vulnerability disclosure interval, average CVSS score, cost of ownership, and a five-star rating representing the vendor’s overall vulnerability posture.

VTEM as well as our Code Maturity analysis (a feature to understand how securely programmed a product is) are just some of the many tools available within VulnDB to allow organizations to fully and properly assess risk.
Case Study: Not A Vulnerability (NAV)

As stated earlier in this report, "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." One way that this manifest is in vulnerability reports that disclose what isn’t really a vulnerability. Due to not properly understanding the issue, or overlooking some aspect that already mitigates it, the researcher claims a program is vulnerable when it isn’t. RBS flags these issues as "not a vulnerability" or 'NAV' for short.

As a vulnerability database, it may seem counterintuitive to track issues that are not a vulnerability. We would prefer not to! However, there are times where the disclosure is not challenged and persists, leaving the bad information available to the public. This could cause an organization that runs across such an issue to waste time trying to determine if they are vulnerable or implement a workaround when it isn’t needed. In those cases, it is better to include such issues but accurately describe the issue and clearly say that it is not a vulnerability.

Generally, RBS policy is to ignore such a disclosure if it is made in one or two places and doesn’t garner much attention. However, when that non-vulnerability is added to another database e.g. CVE, it becomes important for us to cover it properly. This allows our customers to have timely and accurate information about vulnerabilities and non-vulnerabilities, to help better protect their organizations.

To better understand how often this happens, the following graph shows the number of 'NAV' disclosures at the mid-point of each year since 2014, up until the midpoint of 2018. While 2018 currently appears to be less than the two prior years at their midpoints, it still represents a significant number of disclosures that RBS has evaluated and disclaimed as vulnerabilities in order to continue providing the highest quality vulnerability intelligence possible.
### VulnDB vs. CVEID Mid-Year NAV Entries Past Five Years

<table>
<thead>
<tr>
<th>Year</th>
<th>VulnDB Count</th>
<th>CVEID Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>144</td>
<td>19</td>
</tr>
<tr>
<td>2015</td>
<td>178</td>
<td>18</td>
</tr>
<tr>
<td>2016</td>
<td>261</td>
<td>31</td>
</tr>
<tr>
<td>2017</td>
<td>517</td>
<td>159</td>
</tr>
<tr>
<td>2018</td>
<td>188</td>
<td>149</td>
</tr>
</tbody>
</table>
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.