2018 Q3
QuickView
VulnDB

Q3 2018 Vulnerability Trends
Created by Risk Based Security
Issued November 9, 2018
Data as of October 29, 2018

A Small Decrease in Vulnerabilities from All-Time High:
• There were 16,172 vulnerabilities published by Risk Based Security’s VulnDB team through the end of Q3 2018.
• The period up to the end of Q3 2018 showed a 7% decrease over the same period in 2017, which set the all-time high record for number of vulnerabilities.
• Risk Based Security’s VulnDB published 4,823 more vulnerabilities than CVE/NVD through the end of Q3 2018.
• CVSSv2 scores of 7.0+ accounted for 34.9% of all 2018’s published vulnerabilities through Q3.
• Through Q3, 46% of the vulnerabilities not published by NVD/CVE have a CVSSv2 score between 7.0 and 10.
• Coordinated disclosure accounted for 48.3% of 2018 vulnerabilities through Q3. 8.7% of coordinated disclosures were through bug bounty programs.
• Web-related vulnerabilities accounted for 46.0% of 2018 vulnerabilities so far this year.
• Of the vulnerabilities published through the end of Q3 2018, 31.2% have public exploits. 48.4% of 2018 vulnerabilities can be exploited remotely.
• 66.1% of vulnerabilities published through Q3 2018 have a documented solution.
• 3.6% of the vulnerabilities published up to the end of Q3 were classified as SCADA vulnerabilities.
• 3.4% of 2018 vulnerabilities through Q3 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 three quarters 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 by the end of Q3 2018 showed a dip for the first time in recent history. While no significant increase occurred from 2014 to 2016, the number of disclosed vulnerabilities steadily rose until this year. Despite that, RBS reminds report readers that small fluctuations in disclosures happen frequently, and that over time as more sources are examined, that dip may go away entirely. As more scrutiny is given to additional disclosure sources, it can sway the quarterly and yearly totals after initial reports like this one are issued.
The trends through Q3 2018, as compared to 2017, are interesting. Only three months, January (4.5%), February (24.6%), and May (7.6%) showed an increase in disclosures compared to 2017. The remaining months showed decreases ranging from July with a 1.7% dip, to September with a significant 40.0% drop. Again, note that vulnerability aggregation continues after the month has passed. So, while September has come and gone, we still routinely find disclosures from this and prior months as well. That means that in the coming months and years, the total disclosures for September 2018 will rise. For example, in our mid-year 2018 report we reported that "March came in at a significant decrease at the time of this report (-15.30%)", and now March is showing a -13.0% drop. While that is still significant, it demonstrates that these numbers are a moving target over time.
Year To Date through Q3 Comparisons

**VulnDB vs. CVEID Through Q3 Past Five Years**

<table>
<thead>
<tr>
<th>Year To Date</th>
<th>VulnDB</th>
<th>CVEID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>10,162</td>
<td>6,307</td>
</tr>
<tr>
<td>2015</td>
<td>11,445</td>
<td>6,741</td>
</tr>
<tr>
<td>2016</td>
<td>11,741</td>
<td>6,595</td>
</tr>
<tr>
<td>2017</td>
<td>16,984</td>
<td>10,555</td>
</tr>
<tr>
<td>2018</td>
<td>16,172</td>
<td>11,349</td>
</tr>
</tbody>
</table>

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 three quarters 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 vulnerabilities. In today’s hostile computing environment, with non-stop attacks from around the world, organizations using sub-par vulnerability intelligence are needlessly taking on significant risk.

If an organization is unaware of their vulnerabilities, how can they be equipped to act on those posing the greatest risk to their assets? Furthermore, many CVEs are published significantly later than the vulnerabilities in VulnDB.
Year To Date through Q3 2018 CVSS Comparisons

Vuln by CVSSv2 Through Q3

Looking at the CVSSv2 trends for disclosures in the first three quarters of 2018, February continues to have the highest number of critical disclosures (373 or 18.6%), meaning a CVSSv2 score of 9.0 or higher, but September dominates by percentage with 327 or 21.0%. While September has a higher percent of critical issues, February has more in volume. As mentioned in our last report, February can largely be attributed to over 280 critical vulnerabilities patched in Samsung mobile devices, while September had a big spike in Foxit Reader / PhantomPDF that impacted its numbers (96 disclosures). As usual, a majority of disclosures continue to fall in the 'Medium' (4.0 - 6.9) range.

CVSSv2 Scores for 2018 Q3 Vulns Not Published by NVD

46% of vulnerabilities not found in CVE/NVD are scored 7.0 - 10

There are 1,524 vulnerabilities, (High and Severe Risk), that have not been cataloged by NVD. Can you really afford not to know what they are?
Year To Date through Q3 2018 Highlights

Vulnerability Disclosure Path - Q3 2018

- Coordinated Disclosure: 7,807
- Uncoordinated Disclosure: 2,932
- Bug Bounty (Non Vendor): 1,212
- Bug Bounty (Vendor): 190

So far, 48.3% of 2018 vulnerabilities were coordinated with the vendor, a small increase from Mid-year. 8.7% were the result of Bug Bounties.

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

2018 Through Q3 Vulns by Impact Type

- Integrity: 59%
- Confidentiality: 18%
- Availability: 17%
- Unknown: 6%

Of all the vulnerabilities reported in 2018, 59% 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, over 13% 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 1.0%. About 5.8% of vulnerabilities were related to mobile devices, regardless of exploit location.
Of all the vulnerabilities reported in 2018, 43.7% either had public exploits available or sufficient details published to exploit the vulnerability (a working proof-of-concept a.k.a. PoC). Over 12% 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, 24.9% of the reported vulnerabilities currently have no known solution. This underlines that while patching is very important, it cannot be relied on exclusively as a remedy. 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, 67.3% 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's clear 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 many of these issues and significantly reduce the threat from attackers.
Case Study: Third-Party Plugins

Many people are familiar with content management systems (CMS), which are used in a variety of roles. Millions of people use them via hosted software such as WordPress.com and companies use them for blogging and knowledgebase systems. Historically, despite their wide deployment, many of the biggest CMS packages have had relatively few vulnerabilities. For example, since 2012, WordPress has only had 162 vulnerabilities disclosed. Given how prevalent the software is, that number is surprisingly low.

On the other side of the CMS equation are third-party plugins that add an incredibly wide variety of functionality designed to make the core software more effective. WordPress, Drupal, Typo3, and other CMS software offer an expected level of functionality to users. Then, third parties write additional software components to perform added tasks, some of which are used by millions of administrators. These third-party plugins offer an entirely different story when it comes to vulnerabilities.

First, as always, it is important to qualify and disclaim. In this case, third-party plugins can be written by anyone and integrated into the core software. That doesn't necessarily mean the plugin will be used by many people. So, some plugins languish with an extremely limited audience of a few hundred users, while others enjoy more than a million active installations. This is a case where vulnerability statistics are interesting, but may not have any bearing on some users, while being of particular interest to others.

Focusing on two of four examples as seen in the chart below, WordPress plugins appear to receive a lot more scrutiny. While there were only 162 WordPress vulnerabilities in five years, third-party plugins for the software were found to have over 5,000 vulnerabilities. On the other hand, with Jenkins, which is used by corporations much more than individuals, the vulnerabilities in the base software as compared to the third-party plugins are closer in number. Given that some sites, such as those based on WordPress, are compromised via the vulnerabilities in third-party plugins, it is just as critical to stay on top of them as the core software vulnerabilities. How is your organization monitoring the vulnerabilities in third-party plugins? Hopefully your answer is not NVD.

![2012 - 2018 CMS vs. Plugin Vulnerabilities](chartimage.png)
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.