2018 Vulnerability Trends

Created by:
Risk Based Security

Issued February 2019
(Data as of February 7, 2019)

Rise in Vulnerabilities Continues

• There were 22,022 vulnerabilities published by Risk Based Security during 2018, a 6.4% increase or nearly a 1.0% decrease from 2017 depending on perspective. Read on!
• Risk Based Security’s VulnDB published 6,780 more vulnerabilities than CVE/NVD in 2018.
• Vulnerabilities with CVSSv2 scores above 7.0 accounted for 33.3% of all vulnerabilities published in 2018 by VulnDB.
• 45.5% of the vulnerabilities not published by NVD/CVE have a CVSSv2 score between 7.0 and 10.
• Coordinated disclosure accounted for 46.6% of the 2018 vulnerabilities, down a small bit from 2017.
• Web-related vulnerabilities accounted for 47.9% of 2018 vulnerabilities, down a few points from last year.
• 32.7% of 2018 vulnerabilities have public exploits and 50.5% of all disclosed vulnerabilities in 2018 can be exploited remotely.
• 27.1% of 2018 vulnerabilities have no known solution, up 5% from 2017, using current data.
• Almost 8% of 2018’s public vulnerabilities were coordinated through bug bounty programs, an increase from only 5.8% last year.
• 3.5% of 2018 vulnerabilities were classified as SCADA vulnerabilities, double that of last year.
• 27.8% of web-related 2018 vulnerabilities were Cross-Site Scripting (XSS).
Introduction to the VulnDB QuickView Report

The first bullet of the introduction may have offered a head-scratcher for you, and it was designed to do so. More specifically, it was designed to show that perspective and how you interpret numbers can make a big difference. How can vulnerability disclosures in 2018 have represented both a 6.4% increase versus 2017 numbers and a 0.9% decrease at the same time?

Consider that when last year’s report was published, (February 2018), 20,832 vulnerabilities had been identified for the year. Using that number along with the corresponding count of 22,022 vulnerabilities identified to date in 2018, we could say there was a 6.4% increase. However, our standard practice when generating reports is to revisit prior years to pick-up any vulnerabilities disclosed after the report release date. Currently our database includes 22,230 vulnerabilities published in 2017, meaning disclosures attributable to 2017 increased by 6.3% since last years’ report was published. So, depending on the perspective, whether you measure and compare the same time as the report was released each year, or if you measure based on all data available now, you can control the narrative. Either vulnerability disclosures increased 6.4% or there was a 0.9% decrease from last year! As always, RBS strongly recommends that the methodology used to generate vulnerability statistics be disclaimed and explained so that you know exactly what you are reading.

Throughout 2019, we will continue to aggregate vulnerabilities that were disclosed in 2018 but were not noted until the next year. This typically happens in VulnDB as we broaden our source coverage and examine these new sources in a historical context. The number of vulnerabilities disclosed in 2018 will undoubtedly increase by this time next year. RBS has consistently warned that vulnerability statistics are a moving target, and this is a great example. As another example we like to use, as of January 2013, there were 8,822 vulnerabilities disclosed in 2012. Since then, we’ve been checking that total every month. Now? We can say there were at least 10,755 vulnerabilities disclosed in 2012, an 18% increase over the value calculated six years ago. That is why it is so important to aggregate vulnerabilities regardless of their discovery date and according to the disclosure date.

For 2018, the number of vulnerabilities coordinated with vendors accounted for almost half of all disclosures, down 1% from last year. The majority of the vulnerabilities occurred in web-based software — making up almost half of all security issues discovered and reported in 2018. Of those, almost 30% were cross-site scripting (XSS) showing that even basic web vulnerabilities are still prevalent.

While many researchers tend to minimize the risk of some web-based attacks, such as cross-site scripting (XSS), they are still effective attacks. Some of the increase is due to a broader range of software being tested, including a significant increase in software produced in China. In our opinion, the continued migration of applications and functionality to web-based software and services is certainly responsible for much of the increase as well.

The trends in other areas, however, should concern all security professionals. Security software, industrial control software, and programs associated with cryptocurrency are all in vulnerability researchers’ crosshairs. Because of its privileged place and access to most networks and data, any vulnerability in security software should be taken seriously. With over 3% of all vulnerabilities being reported occurring in security software, it sends an important message to vendors that their software must face more scrutiny before release. SCADA vulnerabilities, accounting for 3.52% of all disclosures in 2018, continue to attract attention, and as recent attacks on power infrastructure in the Ukraine and the Middle East have demonstrated, could be very damaging. This represents the highest number of SCADA vulnerabilities in a single year.
Meanwhile, less than half of all vulnerabilities are being shared with the software developers in a coordinated disclosure process. Software developers rely so much on third-party researchers that they need to make sure that outreach is part of the software-security process. RBS frequently observes vendors sternly telling researchers to use a specific disclosure channel, while the procedure is not documented anywhere.

**What Does This Report Cover?**

This report covers the vulnerabilities aggregated by Risk Based Security with disclosure dates between January 1\textsuperscript{st} and December 31\textsuperscript{st} 2018. The information collected is displayed in a series of charts depicting various groupings, classifications, and comparisons of the vulnerabilities. In cases where prior year totals are shown, as well as the 2018 calendar year, the data is based on calculations made as of February 7\textsuperscript{th}, 2019.

This report is designed to provide a variety of observations around vulnerability disclosures in 2018 that can be referenced in your organization.

If you have any questions or suggestions for the next report, please email [RBS Support](mailto:RBS@riskbasedsecurity.com).

We hope you find the report useful!
The number of vulnerabilities cataloged by VulnDB during 2018 was almost identical to the “adjusted” 2017 total, but only after considering over 2,000 additional vulnerabilities from 2017 that were not aggregated until 2018. As mentioned in the introduction, yearly totals are a moving target and we will see an increase as time goes on. Typically, the further from the disclosure year, the slower the total for that year will increase. For example, at the time of last year’s report release date, we reported 14,296 vulnerabilities in 2014, and during 2018, that number only increased by 54, to 14,350. With that in mind, we expect 2018 to be a record high, but it won’t be realized until later in 2019.

As most organizations still struggle to stay on top of the constant flood of vulnerabilities, it is critical that no one takes the numbers above to mean that things are getting better. Organizations must remain vigilant in patching and use this opportunity to consider different approaches to vulnerability management. For example, moving away from a network scanning approach, some organizations are finding that combining vulnerability data with an asset management system is a more comprehensive and timely approach.

Everywhere you look today you see “risk-based vulnerability management” being touted as the next big thing. At Risk Based Security we have been advocates of that concept for nearly a decade. The difference is the data. Calculating a risk score to guide your remediation program, while using incomplete vulnerability information, merely gives you a false sense of security and well-being when perhaps your true risks lie elsewhere. The 1950’s phrase, “Garbage In, Garbage Out”, still rings true. Ask your scanner or security service provider the question, “What is the source of your vulnerability information?” You’ll be surprised at the lack of transparency, meaning they typically rely on CVE/NVD. After you read this report, we doubt you will find that an acceptable response.
CVSSv2 scores for public vulnerabilities have been relatively consistent with about 35% to 40% of the vulnerabilities scoring between 7.0 and 10. With 13.6% of vulnerabilities disclosed in 2018 having a CVSS score between 9.0 and 10.0, organizations must stay vigilant.

Breaking down the CVSS scores further, it is interesting to look at the top 10 vendors with vulnerabilities scored between 9.0 - 10.0. As expected, software with a user-assisted attack vector, such as web browsers, PDF viewers, and Office suites frequently appear on this list. Attacks that require a victim to click on a link or a document that results in code execution, get scored 9.3 per CVSSv2 specifications. In other cases, some corporations suffer due to extremely vague disclosure details in their release. If for example, XEROX publishes a patch and says the patch "fixed a vulnerability", CVSS scoring guidelines
mean you "assume the worse". As a result, they get scored 10.0 even though they may not be nearly as severe.

*Note that the numbers reflected in the chart do not necessarily represent unique vulnerabilities in the vendor products. For example, some XEROX products bundle Mozilla Firefox, and a portion of the Google and Mozilla vulnerabilities are in third-party libraries.*

With the top three products corresponding to personal devices such as cell phones (e.g. Pixel, Nexus, Blackphone SilentOS, Samsung), this chart mirrors a larger and broader trend of such devices becoming more appealing to attackers. As more of the world not only adopts smart phones, but increasingly does business using them, these vulnerabilities will become more prominent and more of a concern.
2018 HIGHLIGHTS

Disclosure Coordination

Note that some vendors do not clearly indicate if a disclosure was coordinated. Further, many researchers will attempt to coordinate with the vendor, but find they are unresponsive and/or take too long to fix the issue. As such, despite an attempt at coordination, some vulnerabilities are disclosed before a fix is available. We’re also seeing a significant increase in coordinated disclosures that make the vulnerability public immediately, as some vendors simply want them filed in a bug tracker like any other issue. The problem with this is obvious.

Disclosure Coordination Trends

<table>
<thead>
<tr>
<th>Year</th>
<th>Coordinated Disclosures</th>
<th>Uncoordinated Disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>28.6%</td>
<td>29.2%</td>
</tr>
<tr>
<td>2015</td>
<td>41%</td>
<td>15.9%</td>
</tr>
<tr>
<td>2016</td>
<td>46.1%</td>
<td>14.3%</td>
</tr>
<tr>
<td>2017</td>
<td>47.7%</td>
<td>19.1%</td>
</tr>
<tr>
<td>2018</td>
<td>46.6%</td>
<td>20.4%</td>
</tr>
</tbody>
</table>

After a three-year increase in coordinated disclosures, 2018 currently shows a small dip. Confirmed uncoordinated disclosures broke 20% this year, reminding vendors that while many researchers are willing to work with them, some simply have no time or interest in doing so. Vendors that have not published a clear disclosure policy should reconsider doing so. Researchers should be given every opportunity to work with a vendor, and the process should be designed for ease on the researcher side, not the vendor.
Bug bounty programs are still a hot topic in InfoSec, and still debated in many ways. While there is a perception that more companies are adopting bug bounty programs, that perception does not match the numbers. The number of disclosures that were part of a bounty program went down just a bit from last year, but that may be partially explained by more service-based companies offering new bounty programs rather than software vendors. Those bounty programs for service-based companies, or government organizations like the Department of Defense (DoD) are out of scope for vulnerability databases.

Vulnerability Impact

The chart above, based on the classic 'CIA' triad model, where risks and vulnerabilities are broken down to those impacting confidentiality, integrity, or availability, is still useful to many organizations. Of all the vulnerabilities aggregated in 2018, 60% affected the integrity of the data in the products. This ranges from various types of data manipulation such as SQL injection to the prevalent cross-site scripting to arbitrary code execution issues.
Exploit Availability

The number of published exploits any given year should be considered as a minimum, as some are published in obscure places, forums that require an account, or without a proper cross-reference to match it to a specific disclosure. Over time, exploits may be written for older vulnerabilities and inserted into vulnerability scanners or published on the web. In other cases, private vulnerabilities may be released later or shared on private forums.

Exploit Location

Almost half of all reported vulnerabilities in 2018 have a remote attack vector (46.9%) followed by about a third having a "context-dependent" attack vector (28.9%), meaning that depending on the implementation of the software, it could require local, remote, or user-assisted vectors. Overall, few of the reported vulnerabilities require some type of physical proximity to a system or device to be exploited, even if they sometimes make big headlines.
A large number of the vulnerabilities reported in 2018 have either updated software versions or some form of patches available (71.1%). However, 27.1% 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 focus on the root cause, which are the actual vulnerabilities, and not solely focusing on the symptoms with patch management. Organizations can make use of detailed vulnerability intelligence to understand prioritization and the ever-changing threats. Note that some patches are in the form of RCS/Git commits and may not be practical for implementation depending on the organization's policy and deployment. Further, 462 vulnerabilities that were reported in 2018 were found to have no risk due to inaccurate disclosures, therefore no solution was necessary.
Of all the vulnerabilities disclosed in 2018, 67.7% 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 software developers still struggle to carefully validate untrusted input. Having a mature SDL that includes secure coding practices can iron out many such issues and significantly reduce the threat from attackers.
Web Related
Vulnerabilities in web applications accounted for almost half of the disclosures in 2018 (47.9%). It should be no surprise that more and more software is being made available as web applications for user convenience. However, with that increased access and ease-of-use, it may open up the field to more would-be attackers. According to Okta, "the number of software apps deployed by large firms across all industries world-wide has increased 68% over the past four years, reaching an average of 129 apps per company by the end of 2018".

Authentication Required
An important aspect of vulnerability exploitation is the access required. In many cases, including 27.5% of the vulnerabilities disclosed last year, that access required some form of authentication. Some vendors will downplay or outright dismiss vulnerabilities that require authentication. In some cases, there are rational arguments as leveraging administrative authentication to exploit a cross-site-scripting issue in a content management system is taking advantage of a feature that is there by design. In other cases, if an account can be self-provisioned or authenticated "guest" access is available, then authentication is not a hurdle at all.

SCADA
Supervisory Control and Data Acquisition (SCADA) software continues to dominate headlines, especially with a recent history of attacks against critical infrastructure around the world. While only 3.5% of vulnerabilities disclosed in 2018 affected SCADA products, that is almost double the disclosures in 2017. Further, it is important to remember that patching SCADA systems is often extremely difficult for a variety of reasons. Even worse, more and more SCADA systems are continuing to migrate to internet-accessible for convenience, without fully considering the safety and security concerns. (See chart on page 14)
Security Software
The hardware and software we purchase and deploy to protect us is becoming increasingly risky. Security-related software from firewalls to anti-virus to intrusion detection and prevention is being found to be increasingly vulnerable. Data from 2018 shows that researchers are taking an increased interest in testing security products, with over 700 vulnerabilities being disclosed. When security companies offer products that claim to "uncover advanced threats and remove false positives" and provide the "ultimate protection against Internet threats", they must be more prudent when it comes to auditing their own code. Further, these vendors should ensure that their response time to reported vulnerabilities is better than the industry average. Given that the very same companies often have their own security research teams that find vulnerabilities in other products, they should be acutely aware of the risk from slow response and long time-to-patch periods.

Vulnerability Dependent
In the same vein as 'authentication required', another important limiting factor in some disclosures is that a vulnerability can only be exploited after a separate vulnerability is exploited first. We are seeing more of these in the last few years as exploit mitigation technologies are becoming more popular. In some cases, we've seen vulnerability / exploitation contests such as "Pwn2Own" prompt researchers to use complicated exploit chains, where a series of three or four different vulnerabilities must be used in tandem to achieve code execution. Some of these disclosures flagged as 'vuln dep', could be minor concerns or weaknesses and not as important to consider. In other cases, if they are part of a fully realized and published exploit chain, that requirement should not be dismissed.

Not A Vulnerability
Over 2% of all "vulnerabilities" disclosed in 2018 were not actually vulnerabilities. At its core, a vulnerability represents a scenario where an attacker can cross privilege boundaries. For 496 of these disclosures, that simply wasn't the case. These disclosures typically explain how the exploit works, but gloss over the fact that they require increased privileges to begin with, and that a user with such privileges could carry out other attacks with similar gains in a far easier manner than outlined in the disclosure. In reality, the number of such disclosures is considerably higher than 496, as RBS does not add every "not a vuln" disclosure to VulnDB. Instead, we only add them when they receive coverage from other vulnerability databases or news articles.

CryptoCurrency
As Blockchain and CryptoCurrency still get a lot of attention in the media spotlight, only 197 vulnerabilities were disclosed in the technology in 2018, impacting consumer software. One aspect of Blockchain technology that is important to note is that in many cases, smart contracts are deployed in a fashion where they are run and are managed on a hosted service platform. That means that vulnerabilities in smart contracts are 'site specific' and outside the scope of most vulnerability databases. If we factored in those smart contract vulnerabilities, we would add 464 more vulnerabilities from 2018!
Vulnerabilities in SCADA products only accounted for 3.5% of all reported vulnerabilities in 2018, up from 1.7% in 2017. It is hard to determine if this significant increase in the number of vulnerabilities found in SCADA products is solely the result of researchers regaining interest and focusing on SCADA products, or if something else is at play. Regardless of the reason, this big jump should cause concern for critical infrastructure administrators, especially as political climates around the world heat up.

The most vulnerabilities disclosed in SCADA products in 2018 were from Advantech Co. Ltd. (21.0%). This was followed by WECON Tech (16%), Schneider Electric (11.5%), Siemens A.G. (8%), and ABB (6.3%).

- 56% of all SCADA vulnerabilities in 2018 were remotely exploitable.
- 76.8% of all SCADA vulnerabilities were related to improper input validation and 3.1% were due to improper authentication management.
While basic vulnerability types have been known for many years, web applications are still riddled with SQL injection and Cross-Site Scripting (XSS) vulnerabilities. These account for almost half of all vulnerabilities reported in web applications in 2018. Despite there being increased awareness and libraries to help sanitize input, these issues remain prevalent.

Organizations producing web-based software can utilize this type of data to better determine what testing is required for their products before shipping. Code auditing and black-box testing must be robust and look for all types of vulnerabilities, not just focus on the higher profile issues like cross-site scripting and SQL injection. While one may think that a remote information disclosure is not as big an issue, such issues certainly can be if they result in the disclosure of user credentials.
The side-by-side view of the total number of vulnerabilities in VulnDB compared to vulnerabilities with a CVE identifier associated with a public disclosure for each year from 2014 to 2018, make it very clear that organizations relying on CVE/NVD or sources and security services solely obtaining data from CVE/NVD are missing an ever-increasing number of the disclosed vulnerabilities. As of February 7th, 2019, VulnDB has cataloged over 65,000 publicly disclosed vulnerabilities that cannot be found in CVE/NVD. These include issues in products from major vendors such as Microsoft, Oracle, Apple, and Cisco, and include a variety of impacts up to and including remote code execution with CVSS scores as high as 10.

The number of vulnerabilities assigned an identifier by CVE/NVD during 2018 was also at an all-time high, mirroring the overall trend. That said, the numbers above reflect the number of CVE IDs that are open and associated with a disclosure during that year. These numbers include the CVE IDs in RESERVED status as well as the CVE ID in REJECTED status.

In addition to the surprising number of missing vulnerabilities, 2018 also saw interesting changes in how MITRE operates CVE. While coverage increased, the quality of the entries significantly decreased. After pressure from the industry and ultimately Congress, MITRE focused on what they call a 'federated' model, calling on CVE Numbering Authorities (CNAs) to rely on vendors and researchers to do more CVE ID assignments than before. Along with that transition, MITRE now allows vendors and researchers to propose the CVE description for a given issue. In the last few months of 2018, it appears that MITRE applied no editorial standards to the entries, and in fact, it appears they didn't even read many of them. That has led to descriptions with simple typographical mistakes as well as others that don't even include the responsible vendor or the impacted product.

This serious decline in quality from MITRE, along with the up to 12-week backlog from the National Vulnerability Database (NVD), means that organizations are getting late and at times unreliable vulnerability information from these two sources, along with significant gaps in coverage. In the past, RBS has maintained that CVE/NVD was no longer "good enough" for your organization’s vulnerability management. Knowing the short-comings with CVE/NVD, can your organization defend its dependency on this information in protecting its assets and the assets of its customers? In our opinion, there is fertile grounds for attorneys and regulators to argue negligence if CVE/NVD is the only source of vulnerability intelligence being used by your organization.
VulnDB vs. CVE/NVD Comparisons

A common misconception or flawed rationale is that vulnerabilities not assigned a CVE identifier must only affect obscure products or are only minor weaknesses. However, as the charts above and below plainly show, many of the “missing” vulnerabilities impact products from major vendors, prevalent products, and have been scored ‘High’ or ‘Critical’ severity. These vulnerabilities are of critical importance to organizations and those solely relying on CVE/NVD for vulnerability data are making risk decisions without the full picture.

Of the 65,000+ vulnerabilities covered in VulnDB that are not in CVE/NVD, many of them are in software made by significant vendors. They span from companies such as Google and key third-party libraries that are integrated into significant projects, to mid-range companies providing software to organizations of all sizes such as Magento, SAP, and Zoho.
One of the common questions we receive after someone hears that we cover over 65,000 vulnerabilities not in CVE is along the lines of "but are they vulnerabilities in software people use?" The answer is a resounding yes. The vulnerabilities cover everything from enterprise software to security software such as anti-virus, from browsers to third-party libraries that can be found in hundreds or thousands of software packages.

Again, everywhere you look today you see “risk-based vulnerability management” being touted as the next big thing. Using incomplete, low quality, and late vulnerability intelligence when calculating a risk score merely gives you a false sense of security. You owe it to yourself to ask your scanner or security service provider the question, “What is the source of your vulnerability information?” Don’t settle for evasive statements or a non-answer.
The Three Biggest Challenges in Vulnerability Tracking

Over the past many years, we’ve observed some changes to how vulnerabilities are being reported. These greatly impact how organizations need to deal with vulnerabilities reported in the products they use as well as the overall value of having access to a vulnerability intelligence solution.

More vulnerabilities are being reported than ever before

As disclosed in our previous VulnDB quarterly and annual reports, the number of vulnerabilities has been steadily climbing each year since 2011. In 2010, a bit less than 10,000 vulnerabilities were reported. This year more than 22,000 vulnerabilities were disclosed. There are various reasons for this increase in numbers including more software being created and a growing focus on vulnerability research.

Vulnerability reporting has become more decentralized

Back in early 2000, an interested organization could generally cover the majority of reported vulnerabilities by monitoring a few mailing lists and a handful of the major vendors’ security pages. For example, years ago the previously popular Full-Disclosure and Bugtraq mailing lists saw hundreds of reports every single month, but they rarely get more than 100 posts a month these days - and sometimes only half of that.

This is a stark contrast to the sharp rise in the number of vulnerability reports. If vulnerabilities are no longer published on mailing lists, where are they being reported? The answer is: “Everywhere and anywhere.” Today, at Risk Based Security we are monitoring thousands of sources ranging from the classic mailing lists and vendor security pages to social media, the deep web, researchers’ own blogs, security companies’ advisory pages, product bug trackers, and commits. And we’re continuously adding new ones!

The quality of vulnerability reports has generally fallen

With so many vulnerabilities being reported and coming from so many different sources, it likely comes as no surprise that the quality of the average vulnerability report has dropped substantially. Poor vulnerability reports are published on a daily basis with various critical inaccuracies and omissions like affected version or references to available fixes. Other reports are simply invalid or duplicates of already known vulnerabilities. What makes matters more difficult and confusing for organizations is that some of these invalid reports and duplicates still end up with CVE identifiers assigned due to insufficient vetting.

There are many reasons for this drop-in quality, but they all ultimately result in the need for a much larger and more costly effort to find and then digest published vulnerability reports.

The vulnerability impact to organizations

Obviously, the three factors above combine to have a great impact to organizations trying to stay up-to-date on the latest vulnerabilities impacting their IT infrastructure. It makes the process much more difficult and resource intensive. Organizations either need to ramp up the assigned resources in their vulnerability management team or accept the risk that they may not be aware of relevant and potentially serious vulnerabilities impacting their assets.

Neither of these two options are great and may ultimately come at great cost.
In the past, while not advisable, it was possible for an organization to at least cover the basics themselves. Today, doing so is simply too costly in terms of the resources and expertise required. It is no longer a question of “can you do it yourself?”, but “why would you even consider doing it yourself?”

The number of scarce and costly resources required for an organization to gather and assess reported vulnerabilities daily is too great when the task can typically be outsourced for less than the cost of a single employee. More importantly, such outsourcing frees up these critical resources for other important tasks necessary to secure your organization’s IT infrastructure.

**The Solution**

Fortunately, there is an option that allows organizations to significantly reduce the internal resources required to gather and process vulnerability information. Utilization of a comprehensive and detailed Vulnerability Intelligence solution such as RBS’ VulnDB allows organizations to focus on adding more value by determining which vulnerabilities could most impact them and how those risks should be addressed.

If you are unsure if your vulnerability intelligence solution is as comprehensive as it should be, you should make it a priority to contact RBS for a demo of VulnDB.

For a complete discussion on this topic, we recommend reading the blog "What You Don’t Know About The Vulnerability Ecosystem Can Lead To A Data Breach" by our Chief Research Officer.

**Methodology & Terms**

Gathering and reporting vulnerability intelligence is not an exact science; but decades of experience helps tremendously. Discovering the new and ever-growing number of sources of vulnerability disclosure is an everyday challenge and processing that information into a usable format requires years of experience, a high-level of expertise, and 24x7 diligence. Incomplete information in the vulnerability source, constant updates and revisions, misinterpretation, and errors in reporting all contribute to a level of confusion regarding the impact, severity, and risk a vulnerability represents.

It is important that vulnerability intelligence and statistics, including those contained in this report, 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. This differs from the reporting of some other 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 publicly disclosed in each period that have an associated CVE ID. This number is lower than the total number of assigned CVE identifiers, which includes around 16,000 RESERVED identifiers that are associated with vulnerabilities that have no published information since CVE began.

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 and perhaps the longevity of your organization may depend on it.
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.

**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.

---

**About Risk Based Security and VulnDB:**

Risk Based Security is a recognized leader in vulnerability intelligence, organizational ratings, and on-demand security solutions. RBS’ mission is to provide action-quality, comprehensive and timely vulnerability intelligence and in-depth organizational security ratings. RBS has developed VulnDB, the largest and most comprehensive vulnerability intelligence database available, to provide customers the vulnerability intelligence to address points of risk across the entire organization – from application development, security operations, vendor risk management and procurement. RBS’ Cyber Risk Analytics, (CRA), the most comprehensive data breach and cyber exposure knowledge base available, supports fact-based procurement due diligence, vendor performance monitoring, organizational ratings, and prioritized remediation for high-risk vendors. Leveraging CRA’s risk ratings with VulnDB’s vulnerability intelligence produces the most comprehensive organization security assessment available. RBS products are available via a SaaS Portal, RESTful APIs, and a customized Alerting system. For more information, please visit:

[https://vulndb.cyberriskanalytics.com/](https://vulndb.cyberriskanalytics.com/)

[https://www.riskbasedsecurity.com/](https://www.riskbasedsecurity.com/)