



**RiskBased  
SECURITY**

# **2021 Mid Year Report**

## **Vulnerability QuickView**



# Welcome

As 2020 unfolded, we noted in our Vulnerability QuickView reports the many factors contributing to heavy disruption to industries and organizations around the world. Those factors include the Coronavirus pandemic, of course, but also the many secondary effects on supply chains, press coverage, investment decisions and more. The disruption to the vulnerability disclosure landscape was seen very early on, in Q1 2020, when we observed a 19.8% drop in disclosed vulnerabilities.

Since then, the vulnerability landscape has somewhat stabilized, as organizations return to something like normal operations. While some of the impacts of the pandemic are likely still in effect, vulnerability trends have rebounded and we are once again seeing growth in disclosures. However, a return to normality isn't always as good as it sounds, especially when it comes to security.

New vulnerabilities are being disclosed every day and important information missed during the pandemic is resurfacing. Organizations may be comfortable returning to their previous processes, but the fundamental problem still remains: there are too many vulnerabilities for many organizations to realistically handle unless they adopt a truly risk-based approach to patching.

We hope that this report helps you move toward implementing a risk-based approach, and gives you a clear picture of the vulnerability landscape. The 2021 Mid Year Vulnerability QuickView Report covers vulnerabilities disclosed between January 1, 2021 and June 30, 2021.

## Key Highlights

- Risk Based Security's VulnDB(R) team aggregated 12,723 vulnerabilities that were disclosed during the first half of 2021.
- The number of vulnerabilities disclosed in the first half of 2021 showed growth of 2.8%, compared to the same period in 2020, despite ongoing business disruptions.
- Of the vulnerabilities disclosed during the first half of 2021, 32.1% do not have a CVE ID, and an additional 7%, while having a CVE ID assigned, are in RESERVED status which means that no actionable information about the vulnerability is yet available in CVE / NVD.
- In the first half of 2021, Risk Based Security's VulnDB team aggregated an average of 80 new vulnerabilities per day. Risk Based Security also updated an average of 200 existing vulnerability entries per day as new solution information, references, and additional metadata became available.
- 1,425 vulnerabilities disclosed in the first half of 2021 are remotely exploitable vulnerabilities that have a public exploit and have a mitigating solution. Organizations should consider fixing these issues as their number one priority if they pose a risk. In addition, Risk Based Security has found an additional 849 vulnerabilities that are remotely exploitable but do not have a mitigating solution.



# In This Issue

## VIEWPOINTS FROM



### Brian Martin

Vice President of Vulnerability Intelligence,  
Risk Based Security

*Brian has been studying, collecting, and cataloging vulnerabilities for twenty-five years both personally and professionally. He has pushed for the evolution of Vulnerability Databases for years via blogs, presentations, and public dialogue on social media, and has helped change them to improve their processes and coverage. He was previously a member of the CVE Editorial Board for ten years and continues to rigorously follow the changing landscape of the vulnerability database ecosystem.*

## WELCOME

<b>Key Highlights</b>	<b>2</b>
<b>Viewpoint</b>	<b>4</b>
Sharks Are Scary but Worry About Mosquitoes	4
<b>Vulnerability Trends in 2021</b>	<b>7</b>
2021 At A Glance	7
“Top” Products by Confirmed Vulnerabilities	8
“Top” Vendors by Confirmed Vulnerabilities	9
Disclosures Over Time	10
<b>Importance of Proper Vulnerability Intelligence</b>	<b>12</b>
<b>In Closing</b>	<b>14</b>
Methodology and Terms	14
<b>Coming Soon: The Risk Based Security Platform</b>	<b>15</b>
<b>About Risk Based Security</b>	<b>16</b>
About VulnDB	16
No Warranty	16

# Sharks Are Scary but Worry About Mosquitoes



## VIEWPOINT by Brian Martin

It seems like every day that we hear about a new hack and read headlines that tell us that so-called advanced persistent threats (APT) are compromising major organizations. These APT and nation-state actors have incredible skill and seemingly an arsenal of zero day vulnerabilities, and apparently no one is safe. Consider them the sharks of the digital criminal world. They are definitely to be feared and certainly fun to read about, as long as it isn't your organization that got popped by one.

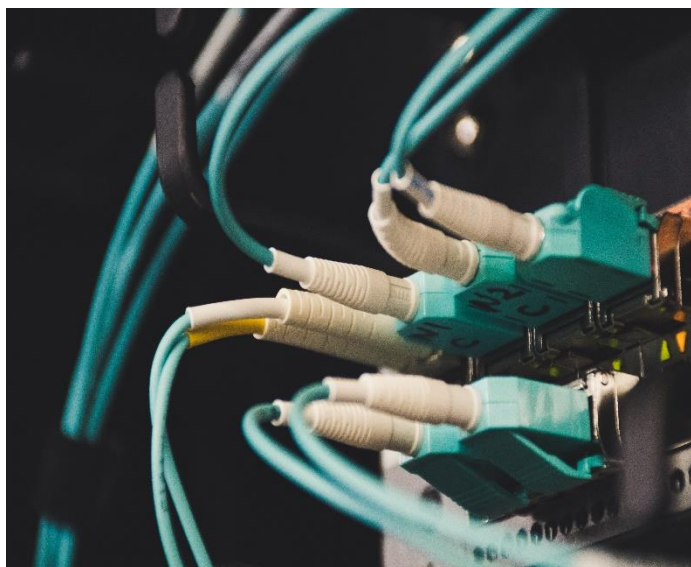
But like those APTs, shark attacks get all the headlines. In reality, [sharks](#) attack very few people worldwide every year and kill even fewer. Instead, it's the [mosquitoes](#) you may need to worry about as they kill over 400,000 every year. Hell, even [hippos](#) who are considered the deadliest land mammal kill more every year, averaging around 500.

But are the numbers the real story here? Partially! If you don't swim in the ocean or live in Africa the odds of you dying by either are essentially nil. So, the numbers give us some perspective on perception of attack and understanding risk. But the analogy breaks down there as any organization is theoretically at risk to the "shark" since they too are connected to the Internet (ocean).

Real-world analogies for computer crime are often good on the surface but break down with casual thought. However, that surface can be beneficial sometimes, like the sharks versus mosquitoes comparison. Instead of using those two as an analogy for the people carrying out the attack, let's use them for types of vulnerabilities instead. Sharks are the zero day vulnerabilities that you have no chance of defending against. Mosquitoes are the tens of thousands of vulnerabilities disclosed every year. In the news now is the attack on Kaseya devices that is being touted as a supply chain attack.







Supply chain attacks have become a hot topic since the [Solarwinds compromise](#) late last year and resurfaced with Kaseya. Are they a threat to your organization? Yes. Are you doomed? Not necessarily. Every company in the world that uses technology relies on both hardware and software from sources out of their control. Pieces of your computer likely come from Malaysia, Indonesia, and Taiwan while software comes from all over the world. Can you trust it? That's a misleading question most of the time because the answer is really in the form of a question: *"Do I have a choice?"* While every organization makes an effort to remain secure, even the biggest can fall victim to computer criminals including [Google](#) and [Microsoft](#).

With more software using some form of automatic updates, the compromise of the parent company may pose a risk to you. However, the alternative is not enabling automatic updates and creating a process to verify those patches before they are deployed. We're not aware of many places that can afford that level of time and expertise to examine every patch before installing it. Even using third-party integrations can be a big concern as we saw with the [Codecov breach](#). You are hopefully aware of that breach since it earned some news cycles, but are you aware that to this day the vulnerability that led to it still doesn't have a CVE ID?

The Codecov supply chain attack was originally assigned CVE-2021-1000009 by the DWF project because MITRE was too slow to assign. However, the DWF project folded again and renamed their IDS from CVE to UVI to be more clear that their assignments are not official CVEs. After that, MITRE still did not assign an ID to this issue which pushed malicious code into organizations. While this is what we would label a hybrid vulnerability, in that it involves a service and software, it is important to include it in vulnerability intelligence. Fortunately for some, MITRE was **only a week late** in publishing an [anemic CVE ID](#) for the Kaseya incident that involved on-prem equipment at customer networks. Days later we [published our first blog](#) summarizing what was known about the Kaseya compromise at the time, in the midst of a lot of confusing and contradictory claims. We [went on to challenge](#) if the incident was really a supply chain attack, while exploring the history of such incidents which actually date back to 1974.

APTs, sharks, hippos, mosquitoes, and a slew of other threats are out there but they aren't all trying to kill you. Cozy Bear, Numbered Panda, Charming Kitten, and SandCat are also threats, but it doesn't mean they are targeting your network. RBS' understanding of this is what makes us the standard bearers for effective Risk-Based Vulnerability Management (RBVM). Devoting too many resources to protecting against the theoretical shark attack, while ignoring the thousands of mosquitos, is probably not the best strategy. Don't lose sight of the daily grind and hundreds of vulnerabilities disclosed every week. They are **annoying, persistent, and can cause trouble** for you just the same. Perhaps that is the real APT.

The Vulnerability QuickView report is powered by



# VulnDB

The most comprehensive, detailed and timely source of vulnerability intelligence and third-party library monitoring.

- ✓ DevSecOps
- ✓ Security & Vulnerability Management
- ✓ Vendor Risk Management
- ✓ Procurement
- ✓ Governance & Management



**REQUEST A DEMO**

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

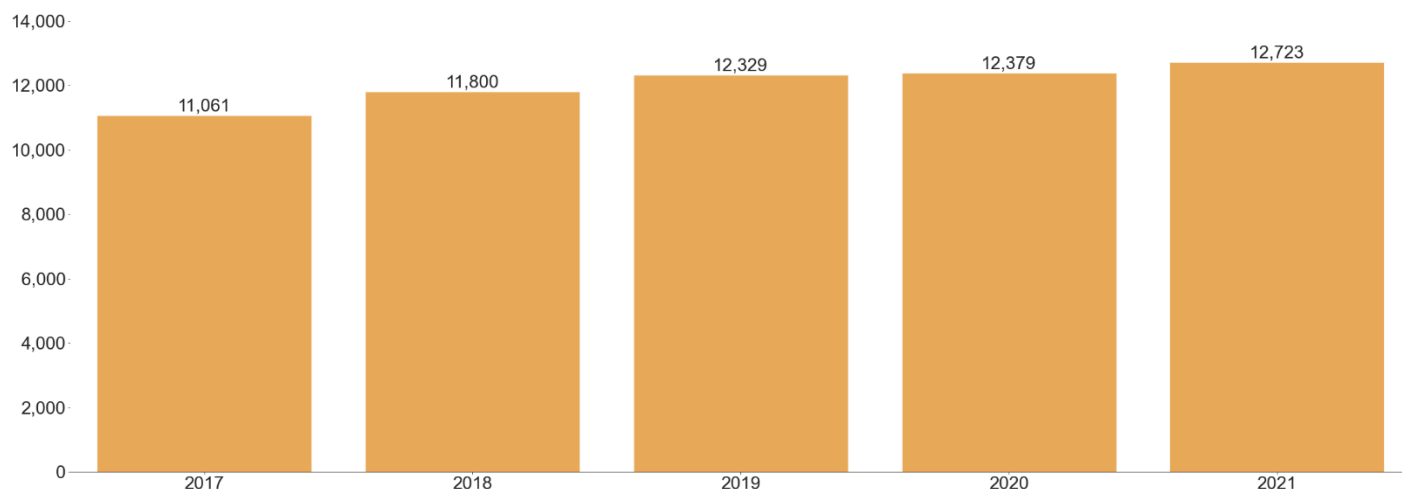


**LEARN MORE**

# Vulnerability Trends in 2021

## 2021 At A Glance

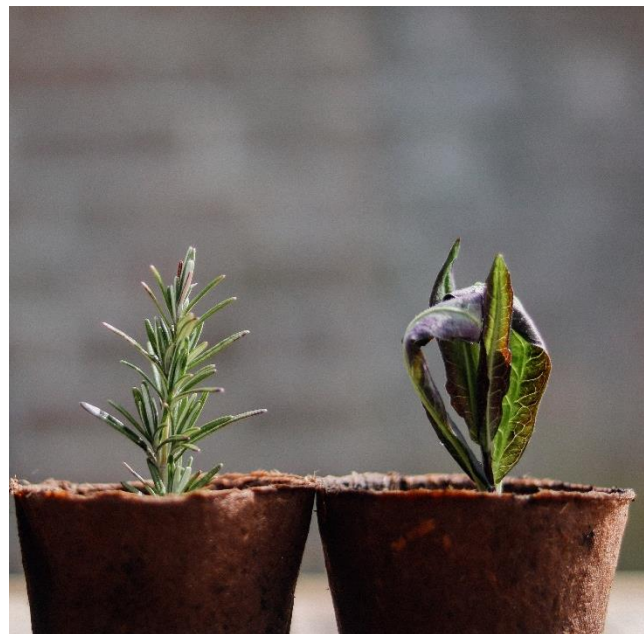
**Figure 1:** Number of vulnerabilities disclosed by Q2, in the last five years



After seeing a [mid-year drop last year](#) during the COVID pandemic, this year has rebounded and brought us back to the vulnerability disclosure trend we're used to seeing; that of growth.







The first half of 2021 saw 344 more vulnerabilities than 2020 at the time of this report, and as we explained in our [2020 Mid Year Vulnerability QuickView Report](#), that number will continue to grow. That post-period growth is the only reason 2020 is higher than 2019 and only marginally so, emphasizing that last year was an outlier.

This year's growth compared to last year is only 2.8%, which isn't that much compared to 2018's growth over the prior year (6.3%), but some of the pandemic related factors that likely led to an initial drop last year may still be in play.



# "Top" Products by Confirmed Vulnerabilities

**Table 1:** Top ten products by vulnerability disclosures in Q2 2021, as compared to 2020.

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Debian Linux	1 	2	628	609
Fedora	2	N/A	584	N/A
openSUSE Leap	3 	1	526	692
Ubuntu	4	4	443	521
Windows 10	5	5	274	478
SuSE Linux Enterprise Server (SLES)	6 	10	260	394
Windows Server (Semi-Annual Channel)	7 	8	259	427
Windows Server 2019	8 	7	248	436
Google Pixel / Nexus Devices	9	9	242	414
SuSE Linux Enterprise Server for SAP	10 	15	233	360

Frequent readers of our QuickView reports should know that this section comes with certain disclaimers. For first time readers, we must disclaim that comparing every product in this fashion may not be statistically correct as not all operating systems are created equal. There are many caveats that can influence a product's spot in our "Which product is the most vulnerable" table such as default configurations, optional software packages, as well as other factors. All of which can either mitigate or eliminate potentially hundreds of vulnerabilities. So please keep that in mind before hastily making conclusions.

Even though vulnerability trends themselves are growing in 2021, this list has stayed relatively the same for a while

now. Debian Linux remains in the top spot since our last report, with Windows Server (Semi-Annual Channel) and Google Pixel staying in place since the year end of 2020. The rest of the listed products have either shifted down slightly or swapped places with other entries.

However, the main difference comes from Fedora. Since our last Vulnerability QuickView Report, our research teams have more specifically delineated Fedora as a distinct product in our database. While this coverage increased the presence of Fedora in the database, it did not represent many new vulnerabilities at all since it shares many of the same utilities and third-party packages as other Linux distributions.



# "Top" Vendors by Confirmed Vulnerabilities

**Table 2:** Top ten vendors by vulnerability disclosures in Q2 2021, as compared to 2020

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
<b>Software in the Public Interest, Inc.</b>	1 <span>↑</span>	8	628	610
<b>Microsoft Corporation</b>	2 <span>↑</span>	3	627	789
<b>SUSE</b>	3 <span>↑</span>	4	590	782
<b>Fedora Project</b>	4	N/A	584	N/A
<b>IBM Corporation</b>	5 <span>↑</span>	6	547	708
<b>Oracle Corporation</b>	6 <span>↓</span>	1	521	915
<b>Google</b>	7 <span>↓</span>	5	503	753
<b>Cisco Systems</b>	8 <span>↑</span>	10	463	384
<b>Canonical Ltd.</b>	9	9	444	522
<b>Red Hat</b>	10 <span>↓</span>	2	439	843

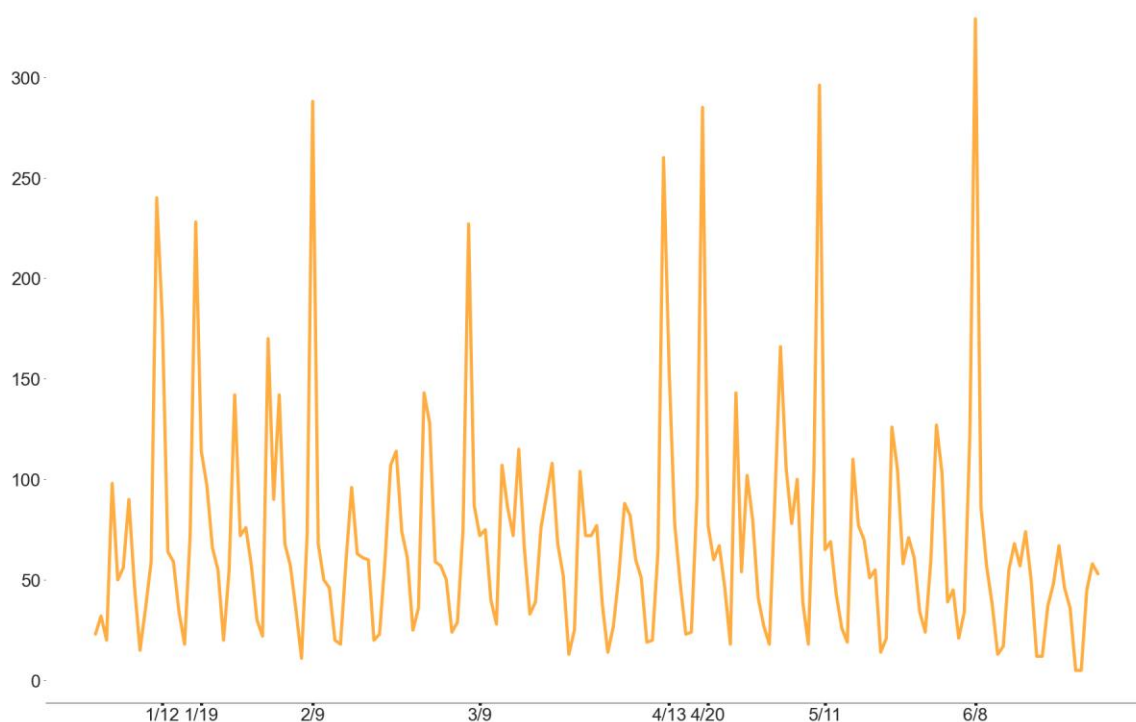
The "top" vulnerable vendor breakdown also comes with similar disclaimers. Like products, each vendor has varied product portfolios, acquisition histories, software development guidelines, install base, bug bounty programs, and more differences that influence vulnerable code. The notoriety of a vendor can also attract vulnerability researchers, who decide what software they will examine.

The top vendors list retains almost all of its 2020 Year End entries, with minor shifting in positions, the only exception being the explicit inclusion of Fedora in our coverage,

adding it to the mix. Having both Fedora and Red Hat on the list is interesting, given the relationship between the two. While Red Hat is the primary sponsor of the Fedora Project, contributions are also made by thousands of other developers. You will notice that Red Hat Enterprise Linux has considerably fewer vulnerabilities than Fedora, and that is due to Red Hat having the luxury of using Fedora as an incubator and testing environment for their own product. Being able to cherry-pick the utilities and new features they include in Red Hat Enterprise Linux allows them to reduce the risk exposure as well.

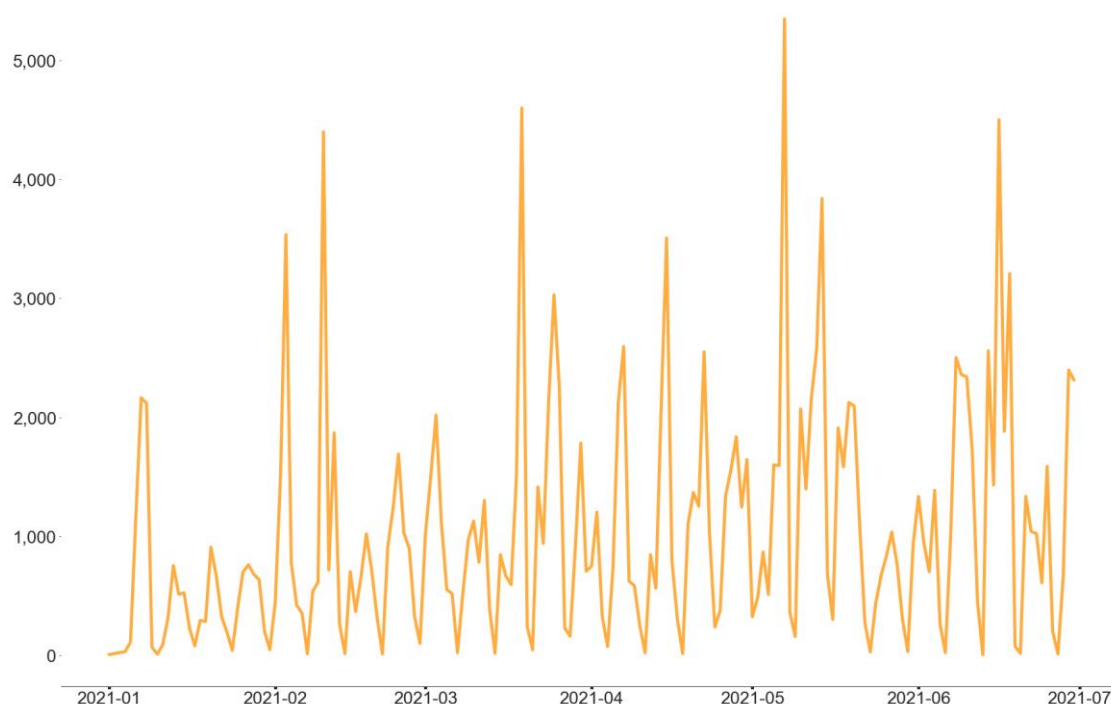
# Disclosures Over Time

**Figure 2:** Vulnerability disclosures each day in Q2 2021, with top days labeled



The first half of 2021 saw ten days with 170 or more new vulnerabilities aggregated by the VulnDB team, with the highest being 329 on June 8. That was a Patch Tuesday that came close to January 14, 2020, the [first of three Fujiwhara events](#) that promised a much higher vulnerability count than it actually delivered. This is a strong reminder that even a “regular” Patch Tuesday has become a serious task

for IT and security teams, as they struggle to implement patches from many high-profile vendors in a very short period of time. As more vendors join the over-crowded Patch Tuesdays, organizations may need to start shifting resources to ensure more coverage around these time periods to help ensure patches are evaluated and applied in a timely manner.

**Figure 3:** Number of existing vulnerability changes each day in Q2 2021

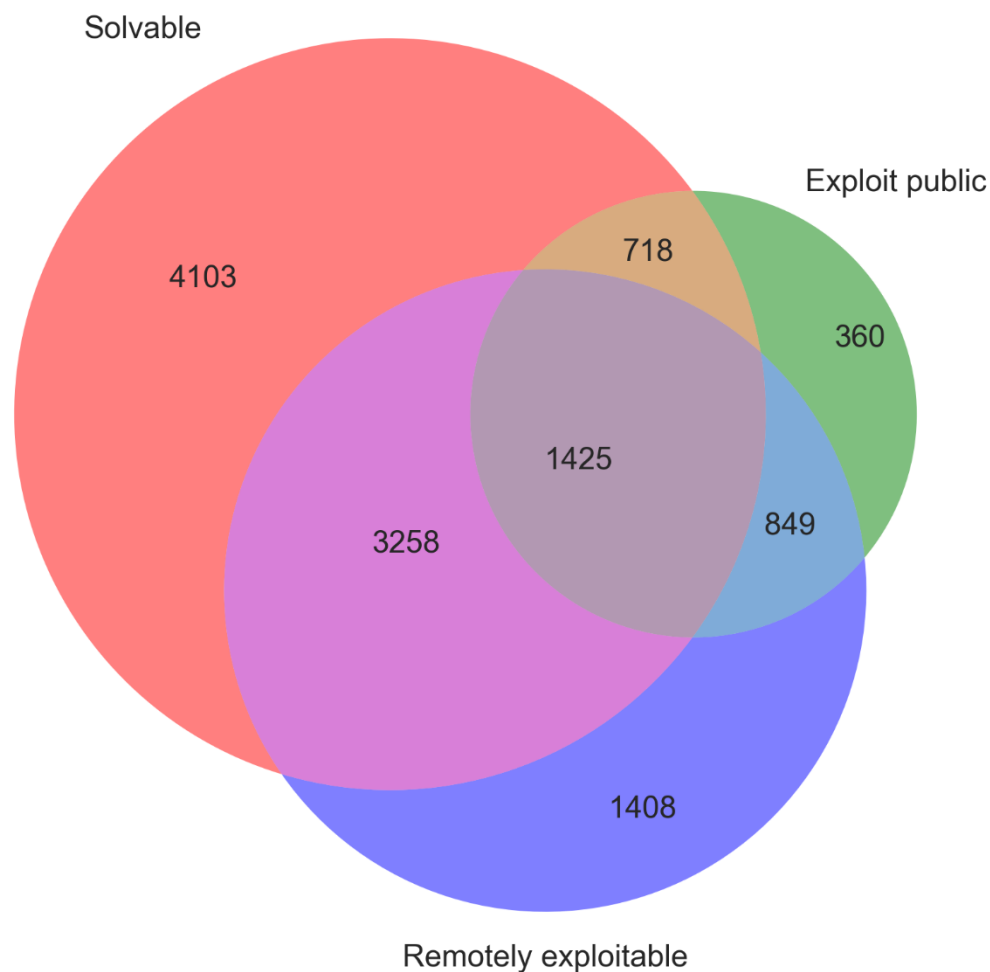
The amount of new vulnerabilities disclosed every day is clearly of paramount importance to organizations, but only slightly behind that are the updates to prior disclosures. It's important to know that some scary new vulnerability is out there posing risk to your assets, but it is also critical to know when a patch for that issue has been made available. While the VulnDB team has averaged just over 80 new

vulnerabilities per day in 2021, the number of updates to existing entries is closer to 200, with the highest day totaling over 6,800 during an import of affected packages for a Linux distribution. These updates range from adding solution or mitigation information, additional products impacted, additional references, clarifications, and more. For a mature vulnerability program, these updates are just as critical as the new vulnerabilities released each day.



# Importance of Proper Vulnerability Intelligence

**Figure 4:** Breakdown of actionable vulnerabilities, by availability and ease of exploitation, disclosed in Q2 2021



Timeliness is a critical component of a vulnerability management program, but making risk-based decisions in an appropriate fashion can be difficult if relying only on publicly sourced data - especially in its basic, unstandardized, and metadata-less form. As seen in figure 4, of the 12,723 vulnerabilities disclosed by mid year 2021,

**1,425** of them are remotely exploitable vulnerabilities that have a public exploit *and* a mitigating solution. As such, organizations should consider fixing these issues as their number one priority if they pose a risk. But if your only source of vulnerability intelligence is CVE / NVD, can you fix these issues in a timely fashion?

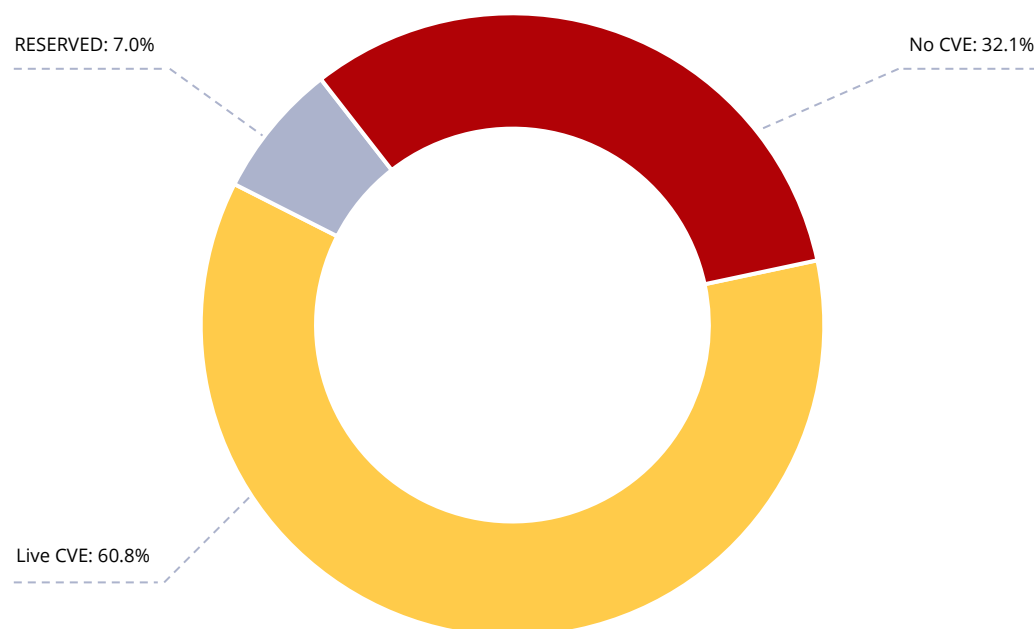
**Figure 5:** Breakdown of vulnerabilities compared to CVE in Q2 2021

Figure 5 showed that within the time period of this report, CVE / NVD missed 4,084 (32%) known disclosed vulnerabilities. An additional 891 (7%) were in RESERVED status, so the number of unactionable vulnerabilities is actually higher since those entries have no detail. Even if the information is there, the exploit status and location within CVE / NVD is not abstracted and requires digging through each disclosure. Given this, what can organizations do? Waiting until vulnerabilities are no longer RESERVED is not a practical option since many of those vulnerabilities remain in that status for indeterminate periods of time. Additionally, since CVE / NVD's information is typically "one-and-done", missing or unreliable exploit and solution metadata will not improve even if a patch is released after the initial disclosure.

So even if the information to fix those 1,425 vulnerabilities is available somewhere, it is not readily accessible to the countless organizations who need to address those issues. To make matters worse, figure 4 shows that there are also 849 vulnerabilities that are remotely exploitable and **do not**

have a mitigating solution. If organizational workflows are already strained from patching vulnerabilities that have known solutions, then adding these vulnerabilities into the mix makes it near impossible for security teams to fully judge risk and secure their assets.

The "patch as many vulnerabilities as you can" culture has been practiced by the industry for decades. However every QuickView Report we release demonstrates that there are simply too many vulnerabilities for an average organization to handle in a timely fashion. To have the best chance of remediating and mitigating the most risk, organizations need comprehensive, actionable and timely vulnerability intelligence. Instead of focusing efforts on increasing the output of patches and basing vulnerability management processes on point-in-time scanning, organizations with limited resources may find more success if they focus on an approach that allows them to prioritize and remediate vulnerabilities via a process informed by their asset context and organizational risk considerations. That is the essence of an effective Risk-Based Vulnerability Management program (RBVM).

# In Closing



The first half of 2021 has shown that the pandemic's unpredictability is fading away. Although the amount of growth in vulnerability disclosures isn't dramatic, it is a clear indication that organizations are returning to a state of normality. But as we go back to the way things were before the pandemic, it makes us question whether or not that is actually good news?

Security teams and vulnerability managers struggled with tremendous workloads long before the pandemic and that will continue to be a problem. Organizations need to find a solution to the main issues their security teams are facing: the ever-increasing amount of vulnerabilities, and the short amount of time they have to effectively remediate those vulnerabilities. Only until those problems are addressed can we begin to see improvements in security as a whole. What is one of the best ways to do that? By using comprehensive, actionable, and timely vulnerability intelligence.

## Methodology and Terms

VulnDB® is derived from a proprietary methodology and daily analysis of thousands of vulnerability sources. Unlike some vulnerability database providers, Risk Based Security is constantly searching for and adding new sources, in addition to working closely with customers to ensure coverage of the products they use.

VulnDB counts only distinct vulnerabilities. Products sharing the same vulnerable codebase are considered only one unique vulnerability. We do not consider vulnerabilities that affect multiple products as unique vulnerabilities as some vulnerability databases do, which artificially inflates their numbers. To be clear, a vulnerability in a third-party library such as OpenSSL is treated as one vulnerability; the multiple projects using and integrating that code do not constitute additional unique vulnerabilities, and are not included in any VulnDB counts.



# The Risk Based Security Platform

Transform your information security program with truly risk-based, asset-centric intelligence.

## REVEAL

the risks that apply to your organization.

## PRIORITIZE

what impacts your assets, products and supply chain.

## REMEDiate

what matters most, coordinating across teams.



Built on the most comprehensive, timely and actionable source of vulnerability intelligence available. Reveal the vulnerabilities that apply to your organization, prioritize, and remediate.

LEARN MORE ABOUT "THE PLATFORM"



# About Risk Based Security

Risk Based Security® (RBS) is a leading provider of Cybersecurity risk management solutions. The award-winning Risk Based Security Platform automatically correlates enterprise IT assets with comprehensive, independently-researched vendor, product and vulnerability intelligence from VulnDB® and Cyber Risk Analytics®. The result is better risk management outcomes, as well as time and cost savings. In addition, YourCISO® provides organizations with on-demand access to high quality security and information risk management resources in one easy to use web portal. Headquartered in Richmond, VA, RBS has been a trusted partner to many of the world's best known brands for more than a decade.

For more information, visit [www.riskbasedsecurity.com](http://www.riskbasedsecurity.com) or call +1 855-RBS-RISK.

## About VulnDB

VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities via an easy-to-use SaaS Portal, or a RESTful API that allows easy integration into GRC tools and ticketing systems. VulnDB allows organizations to search and be alerted on the latest vulnerabilities, both in end-user software and the 3rd Party Libraries or dependencies.

A subscription to VulnDB provides organizations with simple to understand ratings and metrics on their vendors and products, and how each contributes to the organization's risk-profile and cost of ownership.

**REQUEST A DEMO**

[sales@riskbasedsecurity.com](mailto:sales@riskbasedsecurity.com)

**LEARN MORE**

[vulndb.cyberriskanalytics.com](http://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 data breaches. 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.