



**RiskBased  
SECURITY**

+



**FLASHPOINT**

# **2021 Year End Report**

## **Vulnerability QuickView**



# 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.*



### Global Threat Intelligence Team, Flashpoint

*Flashpoint's Global Threat Intelligence team provides organizations with detailed intelligence on malicious actors and their activities on illicit communities. With extensive experience working with commercial and government sectors, the Global Threat Intelligence team specializes in cybercrime and illicit communities, focusing on international segments of the internet, multi-vendor marketplaces, credit card shops, and fraud techniques.*

## 2021 YEAR END VULNERABILITY QUICKVIEW REPORT

<b>Welcome</b>	<b>3</b>
Key Highlights	3
Log4Shell: How "Big" Is It?	4
Log4j Chatter: What Threat Actors Are Sharing About the Log4Shell Vulnerability	8
<b>Vulnerability Trends in 2021</b>	<b>12</b>
2021 At A Glance	12
"Top" Products by Confirmed Vulnerabilities	13
"Top" Vendors by Confirmed Vulnerabilities	14
Disclosures Over Time	15
<b>Importance of Proper Vulnerability Intelligence</b>	<b>17</b>
<b>In Closing</b>	<b>20</b>
<b>About Risk Based Security</b>	<b>22</b>
About Flashpoint	22

# Welcome

Pre-pandemic, the vulnerability disclosure landscape tended to follow the same behaviors year-to-year. Every quarter, vulnerability disclosures would closely match the count from the same period in the previous year. And then, by year end, the total would incrementally exceed the previous year's.

However, in 2020 Q1 we saw a major and sudden drop of 19.8% in disclosed vulnerabilities. Out of all the external factors, COVID-19 was the most likely underlying cause, though nothing could be specifically attributed to the pandemic. Since then, while the total vulnerability count has steadily caught up over the past two years, COVID always appeared to influence the numbers.

Now that we have a full picture of 2021, it looks as if the vulnerability landscape has truly returned to normal. And while the normalization of the space may seem comforting, for struggling organizations it is not. Vulnerabilities have increased by a noticeable margin, and 2021 can now be credited with the most disclosures on record.

There are too many vulnerabilities for organizations to remediate all of them, and they are being disclosed too quickly for organizations and security teams to keep up with. As usual, this includes CVE / NVD. In a world where issues like Log4Shell can appear at any time, organizations need proper vulnerability intelligence in order to make risk-based decisions. We hope that this report demonstrates why Better Data Matters® as organizations strive to make those decisions.

The 2021 Year End Vulnerability QuickView Report covers vulnerabilities disclosed between January 1, 2021 and December 31, 2021.

## Key Highlights

- Risk Based Security's VulnDB® team aggregated 28,695 vulnerabilities that were disclosed during 2021. That total is the highest number on record.
- Spikes of vulnerability disclosures are occasionally occurring outside of routine 'Patch Tuesdays', with one such event resulting in 287 vulnerabilities released in a single day.
- 4,108 vulnerabilities disclosed in 2021 were remotely exploitable, with both a public exploit and documented solution information. By focusing on these issues first, organizations can potentially reduce their risk and immediate workload by nearly 86%.
- Of the vulnerabilities disclosed during 2021, 29% do not have a CVE ID, while an additional 4% have a CVE ID assigned but are in RESERVED status. This means that no actionable information about the vulnerability is yet available in CVE / NVD.
- CVE / NVD's inability to report on 33% of 2021's vulnerabilities results in a loss of visibility for organizations seeking to replicate the best practice of focusing on remotely exploitable vulnerabilities that have a public exploit and also a documented solution.

# Log4Shell: How “Big” Is It?

**VIEWPOINT** by Brian Martin

By now, the entire world is hopefully aware of what [Log4Shell](#) is, and why it’s a major problem. Since its [discovery at the end of November last year](#), the news has been dominated by headlines touting its impact and how organizations need to pay attention, stop, and remediate Log4j issues. While more and more articles are published, each of them seems to be asking the same question, but they all seem unable to give a clear answer: *Just how “big” is Log4Shell?*

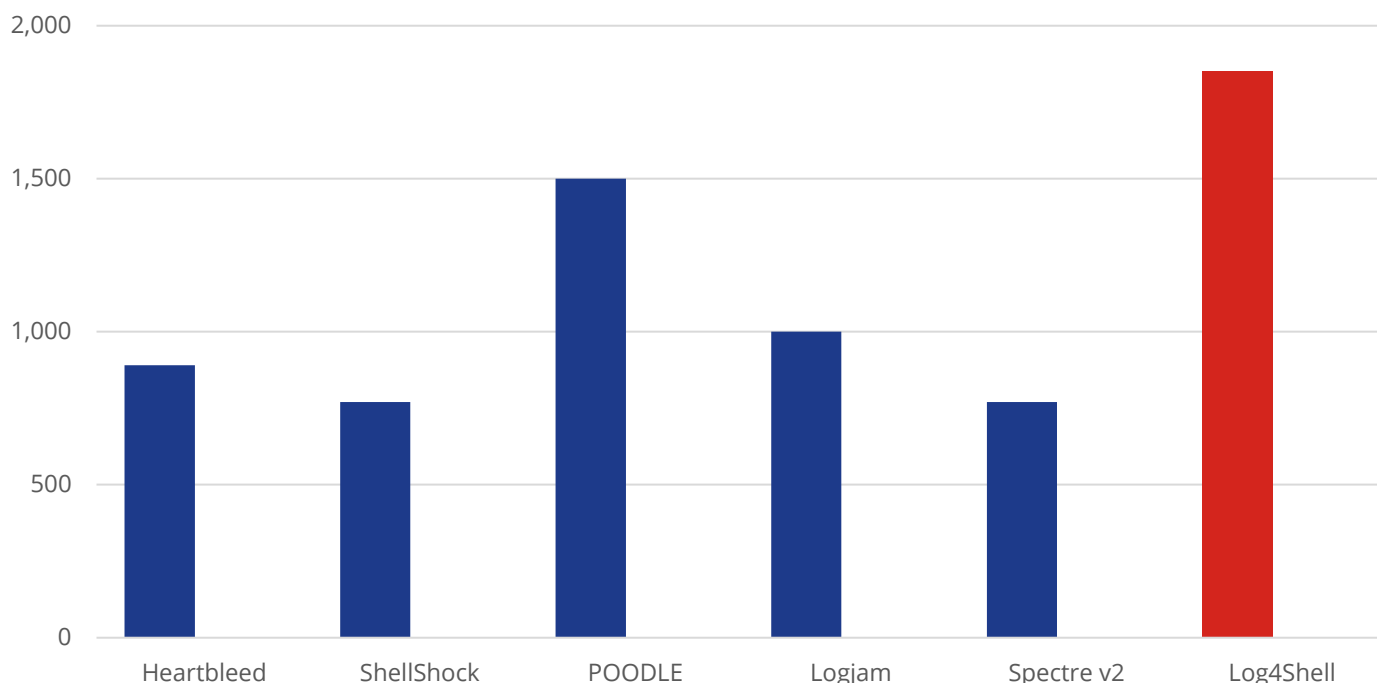
## LOG4SHELL IS A MEGA-VULNERABILITY

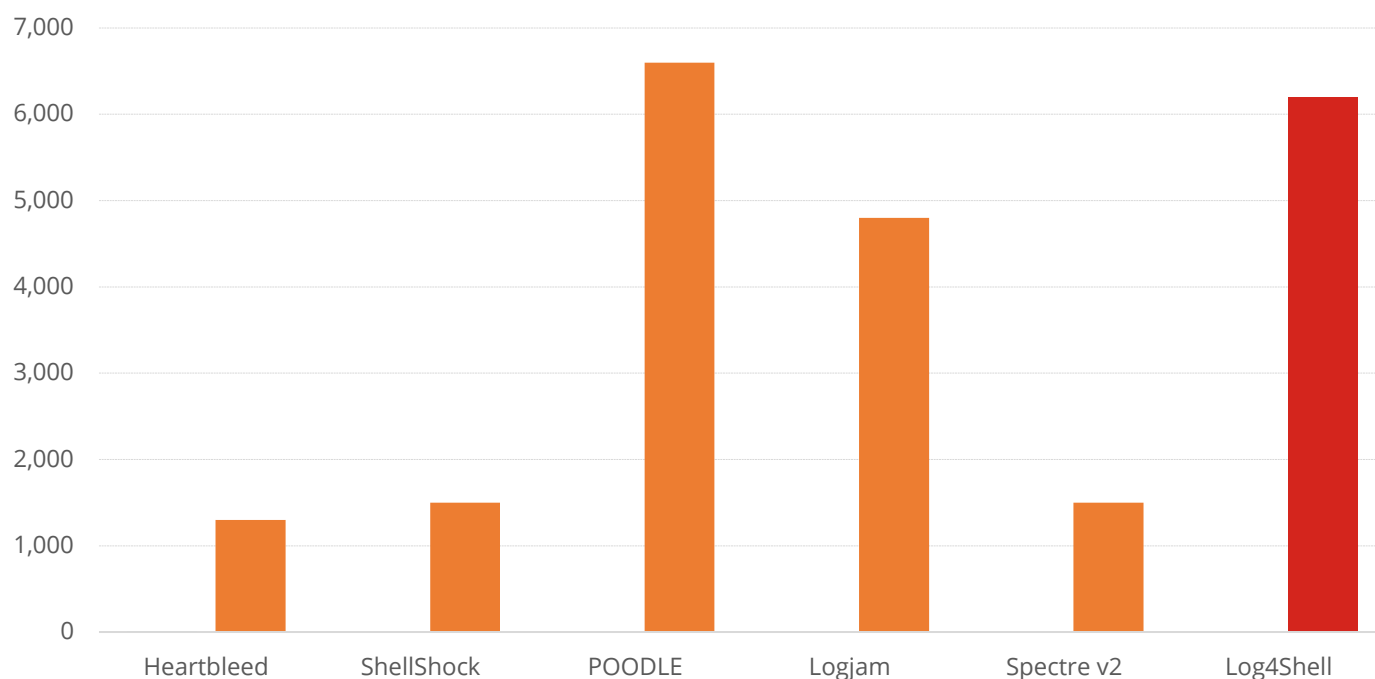
If you are not familiar with what we do at RBS, or what [VulnDB](#) is, we can start with the fact that it is the most comprehensive, detailed, and timely source of vulnerability intelligence available on the market. That means the data that we provide our customers is independently aggregated, containing vulnerabilities found in IT, OT, IoT, CoTS, and third party libraries and dependencies.

VulnDB details over 280,000 vulnerabilities, including over 91,000 that CVE/NVD fails to report. This context helps us fully explain and contextualize Log4Shell’s size and impact, since it has become what we call a “mega-vulnerability”.

This term describes entries that take up significant bandwidth in our database, and notable “mega-vuln” entries include [Spectre](#), [POODLE](#), and [Heartbleed](#). At first glance, it may seem that there’s a correlation between size and infamy, but the amount of attention a vulnerability receives is not the defining factor. Rather, to qualify as a mega-vulnerability, entries need to have hundreds or even thousands of vulnerability references while affecting a tremendous amount of products and vendors. The accompanying charts illustrate how Log4Shell compares among its peer group.

**Figure 1:** Total number of vulnerability references for mega-vulnerabilities



**Figure 2:** Total vendors/products affected by mega-vulnerabilities

### LOG4SHELL'S UNPRECEDENTED GROWTH

Most mega-vulnerabilities take years to accumulate references and affected vendors/product information. But in just a month, Log4Shell has surpassed every other mega-vulnerability, except for one. At this time, there are over 1,850 vulnerability references specifically citing Log4Shell and its variants, and they affect over 6,200 vendors/product combinations. Of those, over 275 are unique vendors and 1,677 unique products, meaning that some organizations will likely be impacted several times over.

In terms of affected vendors and products, Log4Shell falls slightly behind POODLE. However, if Log4Shell-related vendor advisories continue at their current pace, it will likely surpass POODLE within the next month. Nevertheless, the main highlight is the incredible amount of Log4Shell references circulating on the web.

Out of all 280,000 known vulnerabilities, Log4Shell has the most references by a wide margin. This means that there is an incredible amount of existing information out there. But if that's the case, why are organizations seemingly struggling to mitigate and remediate affected assets?

## VULNERABILITY REFERENCES PROVIDE A CLEARER PICTURE OF RISK

Despite the plethora of available information, organizations typically don't have a tool that aggregates every known reference in one place. Vulnerability references provide much needed context for an issue, making it essential for intelligence vendors to constantly update their entries (especially Log4Shell) with as many of them as possible.

Even though they should, most vulnerability intelligence vendors do not do this. References can contain new information that could drastically affect the impact, severity, or solution availability for a given vulnerability. It's common to see a vulnerability disclosed that does not initially have every detail needed to properly triage it. Key details like location, exploitability, or solution information are often found after the vulnerability's initial disclosure, and they can come from third-party sources that are unrelated to the originating vendor.

As such, vulnerability references play a critical role in contextualizing the risk that an issue poses to organizations. By taking advantage of a feed that captures them and includes them with the actual vulnerability entry, organizations will be better informed if they need additional details specific to a vendor or product. Without references, security teams may question the provenance of the information in the vulnerability database. And when it comes to Log4Shell, security professionals don't have the resources to scour the internet for every mention.

But depending on where you get your vulnerability data, hours spent researching Log4j issues will only scratch the surface. This is especially true if using publicly sourced data from CVE/NVD:

CVE-ID	
<b>CVE-2021-44228</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> <li>CERT-VN:VU#930724</li> <li>URL:<a href="https://www.kb.cert.org/vuls/id/930724">https://www.kb.cert.org/vuls/id/930724</a></li> <li>CISCO:20211210 A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021</li> <li>URL:<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a></li> <li>CISCO:20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021</li> <li>URL:<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a></li> <li>CISCO:20211210 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021</li> <li>URL:<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a></li> <li>CONFIRM:<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf">https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf</a></li> </ul>	



Although CVE disclaims that its list of vulnerability references should not be considered complete, in the end, what is provided simply doesn't benefit the end user. On the other hand, VulnDB catalogs over 1,850 Log4Shell references compared to MITRE's list of around 100, meaning that CVE/NVD users will be forced to find as much as 95% of the information that is actually available themselves.

## THE IMPORTANCE OF STANDARDIZED DATA

Some skeptics may argue that providing every reference could actually just overload security teams instead of providing a benefit. And in the age of overwhelming amounts of data, this concern has merit. If we were to dump every known reference on organizations without validating their value, the sheer amount of data may render the information unserviceable. But what if every vulnerability reference was sorted based on their contents and relevancy, with options to consume based on affected CPEs?

This is the importance of an independently researched, comprehensive, and detailed vulnerability database. By being proactive in searching and capturing published details, we are able to provide organizations with a more complete picture, allowing security professionals to make informed risk-based decisions.

# Log4j Chatter: What Threat Actors Are Sharing About the Log4Shell Vulnerability

## VIEWPOINT by Flashpoint's Global Threat Intelligence Team

Since the Apache Log4j disclosure in December, organizations are feverishly attempting to identify and patch all potential vulnerabilities to their systems and infrastructure. In the meantime, threat actors across various illicit communities are actively discussing ways to exploit and further monetize this vulnerability.

Below, we break down the most significant chatter amongst threat actor groups, with a particular focus on deep and dark web forums XSS, Raid, and RAMP.

## THE CHATTER ON XSS

In December, just a few days after the vulnerability was published, Flashpoint analysts identified a thread on the top-tier Russian-language hacking forum XSS titled "CVE-2021-44228 Apache log4j RCE", in which threat actors actively discussed Log4Shell-related activity, including:

- Information sharing on proof-of-concept (PoC) exploits for Log4Shell
- Contributing to mapping out the Log4Shell attack surface
- Providing information on how to scan for systems vulnerable to Log4Shell
- Web application firewall (WAF) evasion payloads
- Sharing information on how to bypass Cloudflare protections to deliver a Log4Shell exploit payload
- Sharing updates on patch releases for Log4Shell

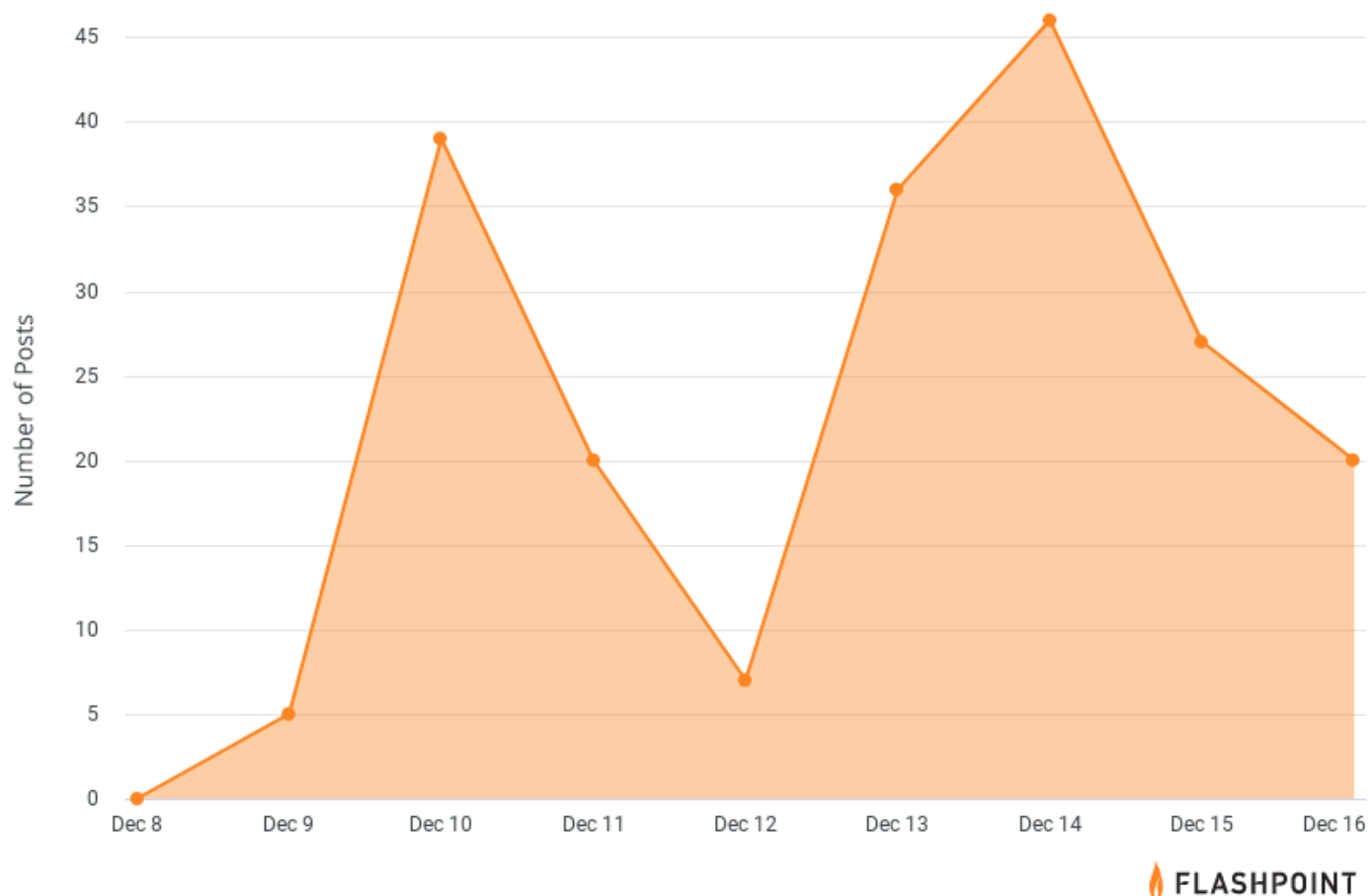
## LOG4J AND GITHUB: HOW THREAT ACTORS WEAPONIZE OPEN-SOURCE CODE REPOS

The majority of the information shared in the Log4Shell-related XSS thread identified by Flashpoint is derived from GitHub repositories. GitHub initially removed repositories containing PoC exploits for Log4Shell to give administrators extra time to patch, given the severity of the vulnerability. Threat actors on XSS were quickly aware of this and in response, posted cloned GitHub repositories containing Log4Shell PoC exploits before GitHub had the opportunity to remove them.

This activity demonstrates a clear intersection between GitHub and cybercriminal communities. GitHub repositories remain a primary resource for threat actors, even amid GitHub's attempts to remove repositories containing malicious artifacts.



## Posts Containing GitHub Links to Log4Shell-Related Repos



### RAID FORUMS

Threat actors on the English-language illicit community Raid Forums were actively involved in propagating the following information related to Log4Shell:

- New plugins for popular vulnerability scanning tools tailored toward identifying systems vulnerable to Log4Shell
- Custom tools designed to scan for systems vulnerable to Log4Shell
- PoC exploits for Log4Shell

Raid Forum admins were aware that chatter about Log4Shell would likely bring increased attention to the forum by law enforcement and press. As a result, Raid Forum admins consistently removed threads containing information related to Log4Shell. However, similar to GitHub, threat actors on Raid quickly downloaded shared PoC exploits and tools before admins had the opportunity to remove them.

## RAMP

On December 11, within the general chat box of the ransomware forum RAMP, several threat actors said they had not heard from the ransomware group “LockBit” for a while. One individual stated that LockBit is working on Log4Shell but did not provide details about the type of work the ransomware collective is allegedly conducting.

Notably, LockBit’s spokesperson on RAMP often openly criticizes RAMP admins, referring to the forum as a “cop forum.” While the aforementioned comment could be a joke, Flashpoint has continued to actively monitor RAMP for any further information.

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/)

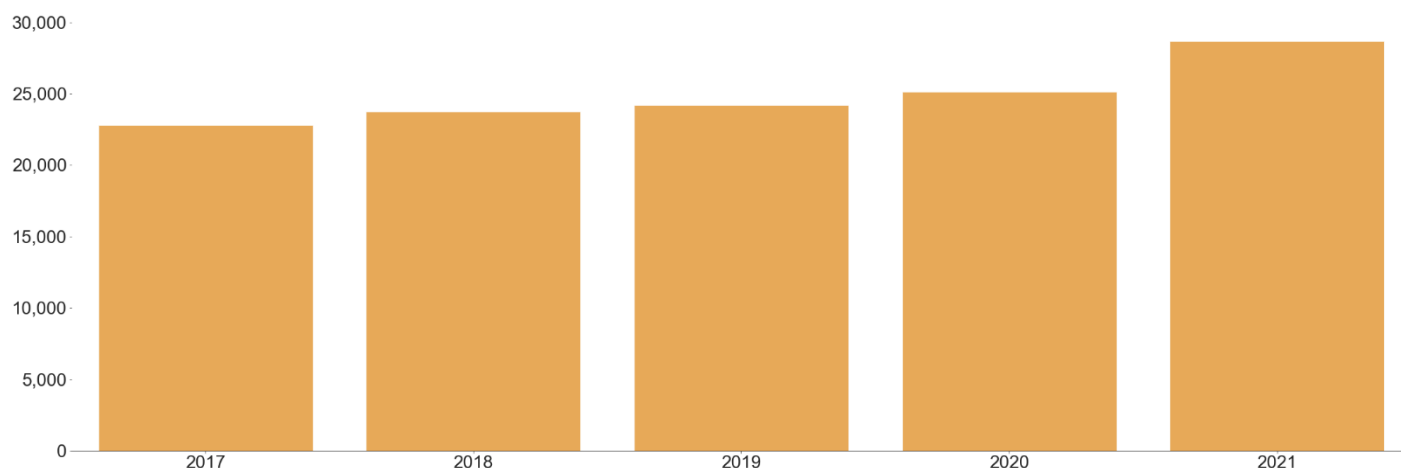


**LEARN MORE**

# Vulnerability Trends in 2021

## 2021 At A Glance

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











For two years, COVID has had an observable, yet uncertain impact on vulnerability disclosures. However, 2021 year end data suggests that the vulnerability landscape is officially returning to normal. While there are many variables that may impact the number of vulnerabilities disclosed, in our [previous reports](#) we theorized that several pandemic factors likely caused a decrease from what is usually seen in similar periods.

Since then, a full view of 2021 shows that the total of new vulnerability disclosures has risen significantly in just the latter half of the year. Although not definitive proof, the major jump of disclosures suggests that COVID truly had influenced the numbers. It is easy to imagine that with changes from working in office to working from home, formerly disruptive routines have now become normal. Considering how security professionals have mostly adapted to their new environments, as well as the standard increases we tended to see pre-pandemic, 2021's jump makes sense. With at least 28,695 vulnerabilities disclosed last year, 2021 has the highest number on record so far.

However, the most interesting aspect to 2021's total is the short time it took to exceed previous years. In the [2021 Mid Year 2021 Report](#), the difference between 2020 and 2021 was only around 400. In the second half of the year, that gap then increased by over 3,500. This is a considerable increase, further lending to the idea that we are seeing the disclosure landscape shake off the pandemic as researchers return to their normal output.

## “Top” Products by Confirmed Vulnerabilities

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

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Debian Linux	1 	2	1,218	1,235
openSUSE Leap	2 	1	1,178	1,275
Fedora	3 	7	995	822
Ubuntu	4	4	847	1,039
Google Pixel / Nexus Devices	5 	12	738	757
Oracle Linux	6 	7	627	869
Red Hat Enterprise Linux for Power	7 	13	591	746
Red Hat Enterprise Linux for IBM z Systems	8 	15	577	725
Red Hat Enterprise Linux for x86_64	9 	5	571	992
SuSE Linux Enterprise Server (SLES)	10	10	570	794

In what has become a common pattern every year, the same 12 - 15 products jockey for position on the “Top Products” chart. For those unfamiliar with this report, it is important to remind readers that these numbers are interesting in terms of volume, but should not be the basis for any product comparisons or assessments. With that in mind, there is a significant change in 2021 that stands out: no Microsoft Windows products!

## “Top” Vendors by Confirmed Vulnerabilities

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

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
IBM Corporation	1 ↑	5	1,321	1,457
SUSE	2 ↑	4	1,280	1,497
Google	3 ↑	6	1,254	1,388
Oracle Corporation	4 ↓	1	1,249	1,728
Microsoft Corporation	5 ↓	2	1,245	1,593
Software in the Public Interest, Inc.	6 ↑	7	1,243	1,236
Dell	7 ↑	8	1,115	1,205
Red Hat	8 ↓	3	1,081	1,516
Fedora Project	9 ↑	10	995	822
Canonical	10 ↓	9	853	1,040

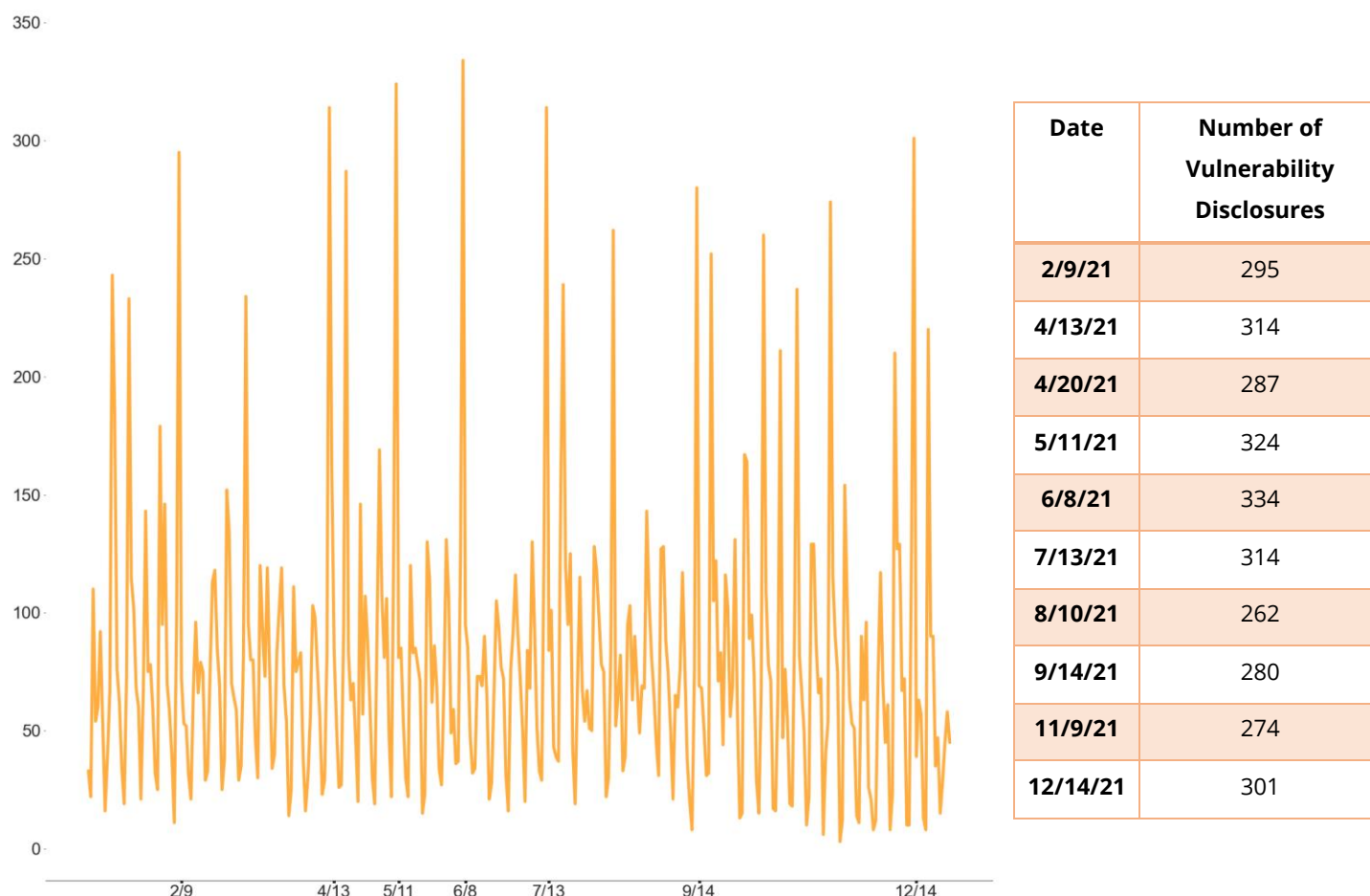
Continuing the thought from the previous section, in 2019 we didn't include a top product chart, but Microsoft was number seven on the top vendor list. Then in 2020 four Windows products occupied the Top Ten list. Now that there are no Windows products present on the Top Ten list, have Microsoft vulnerabilities dropped in 2021? The answer is a resounding yes. However, 2020 was an unusually bad year for Microsoft, jumping from 944 to 1,593. If 2020 was an abnormally bad year for Microsoft, then seeing a drop in 2021 would be expected. That, along with a steady increase in vulnerabilities affecting products from other vendors, would explain the absence of Microsoft Windows from the product chart above.

With the 2021 top vendor chart, we see that despite the drop in Microsoft vulnerabilities, they still reached the number five spot. That tells us that while there were a considerable amount of vulnerabilities in their products, not one Microsoft product managed to reach the Top Ten. IBM also experienced this, being number one on the top vendor list while having no products make the Top 10 Product list. The reason is simple: for organizations with a sizable product portfolio, the distribution of vulnerabilities per product evens out and leads to a more nuanced take. Therefore, rather than assuming companies like IBM or Oracle are “the worst vendors” based on their overall vulnerability count, it is crucial to look closer at the product(s) deployed in your organization. Those product-specific totals will be of more practical use. Further, depending on the quality of your vulnerability intelligence, having access to detailed metadata will be extremely useful in developing specific and contextualized metrics for your security teams.



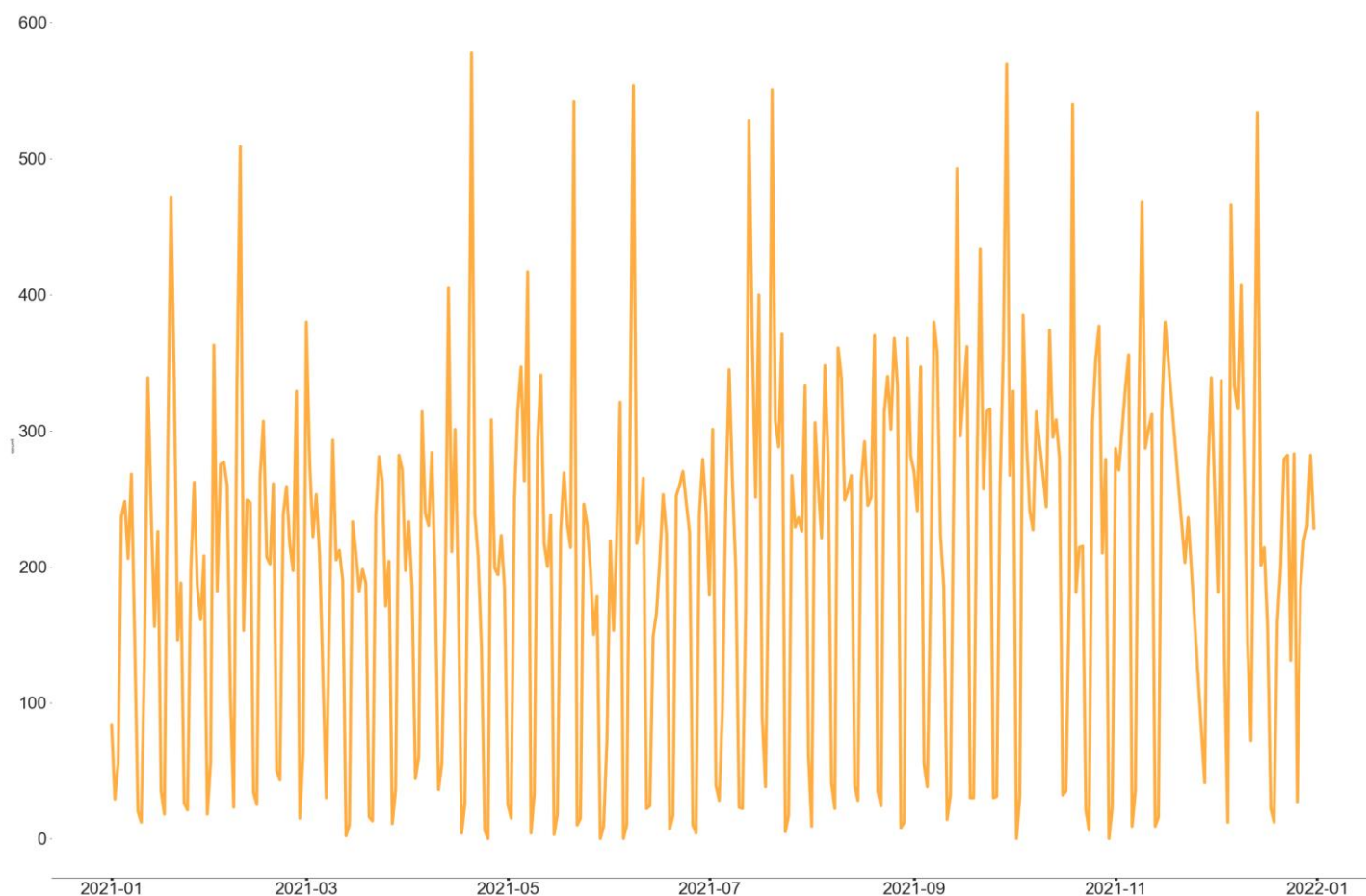
## Disclosures Over Time

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



Looking at 2021 over the full year, we can track disclosures by day. In the grand scheme of things, we know there is volatility in disclosures due to some vendors opting to follow 'Patch Tuesday', where they release patches on a given day of the month. This chart highlights just how severe that practice has become and the burden it can place on security teams even though it occurs at fairly regular intervals.

However, this chart shows that there are also unexpected surges of disclosures. Notably, April 20 is not a 'Patch Tuesday' but had 287 disclosures putting it the 7th highest for the year, ahead of some Patch Tuesdays. Conversely, we see that disclosures on any given day in January didn't make the top ten days. Preparing for the usual days is important, but security teams must stay fluid and be ready to respond to high disclosure days that are 'out of band'.

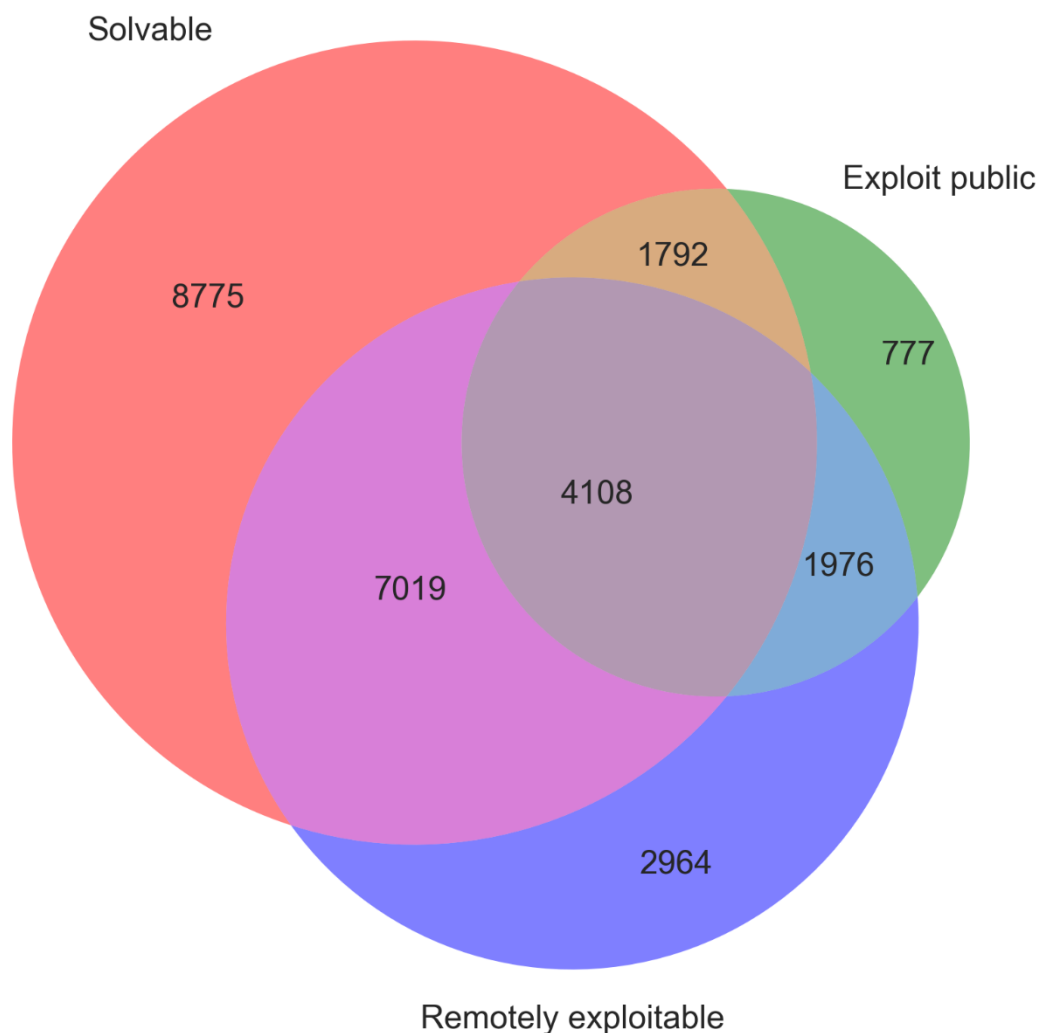
**Figure 3:** Number of existing vulnerability changes each day in 2021

We have talked about the concept of a “[living database](#)” before, and the updates made to VulnDB continue to demonstrate the value of that approach. If you’re not familiar with the concept, it refers to our belief that vulnerability databases should be constantly revisited and updated as new details come to light. This graphic shows the number of daily updates made to VulnDB entries. These changes range from adding a reference to adding additional affected products or including a newly released solution.

Updating previous records is vital because if a vulnerability is disclosed and isn’t coordinated with the vendor, it can be days, months or even years before a solution is made available. While your organization may have introduced mitigating controls, it is still extremely important to install the patch or upgrade when it becomes available. Relying on a “one and done” vulnerability database is not likely to help. While such a solution may provide the original information available at the time of initial disclosure, if it is not updated with subsequently available remediation information then your organization is missing out on crucial data needed to truly mitigate vulnerability-related risk.

# Importance of Proper Vulnerability Intelligence

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



We've included the actionable severity chart in our past two reports, as well as in our monthly QuickView Infographics for a simple reason - it succinctly demonstrates the value of quality vulnerability intelligence. Expecting any organization to triage, prioritize, and then remediate 28,695 vulnerabilities in one year is extremely unrealistic, and without a risk-based approach, key issues are more likely to remain unpatched.

To make the most effective use of time and resources, security teams should first focus on issues that are remotely exploitable, have a public exploit, and have documented solution information. By following this approach, organizations can focus on the 4,108 vulnerabilities that fall into this category, potentially reducing their immediate workload by 86% while still addressing the most significant risks with which they are faced. This allows organizations to make an informed decision on how to prioritize the other 24,587, since vulnerabilities with all three stipulations will likely have the most impact, while being the easiest to remediate. However, even though this best practice can bring tangible improvements to the timeliness of any organization's Vulnerability Management Program, if your vulnerability intelligence is poor, or is publicly sourced, this model may be theoretical at best.

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

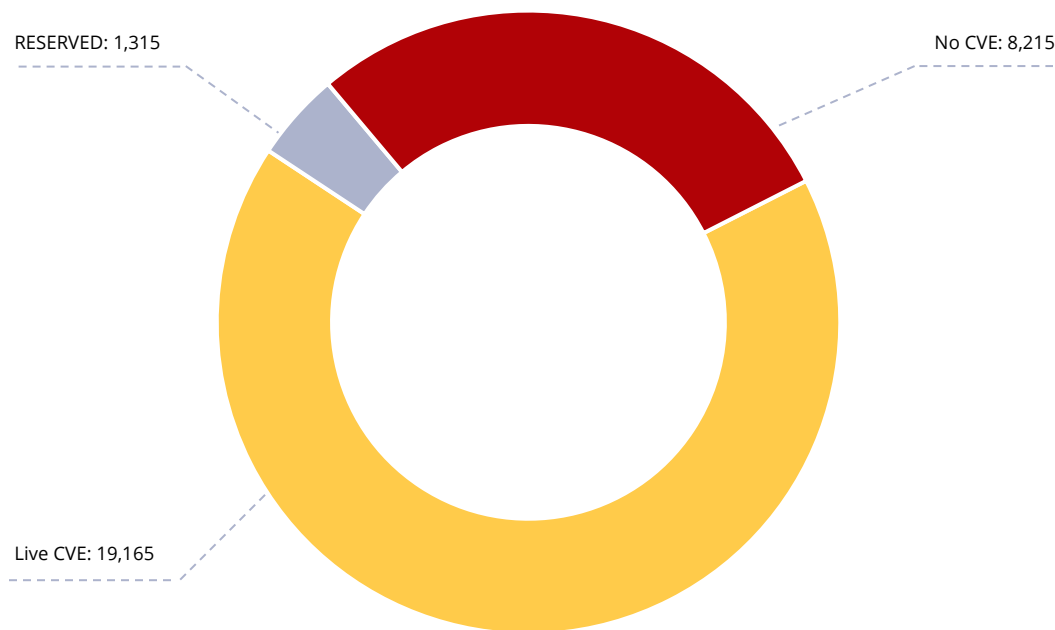
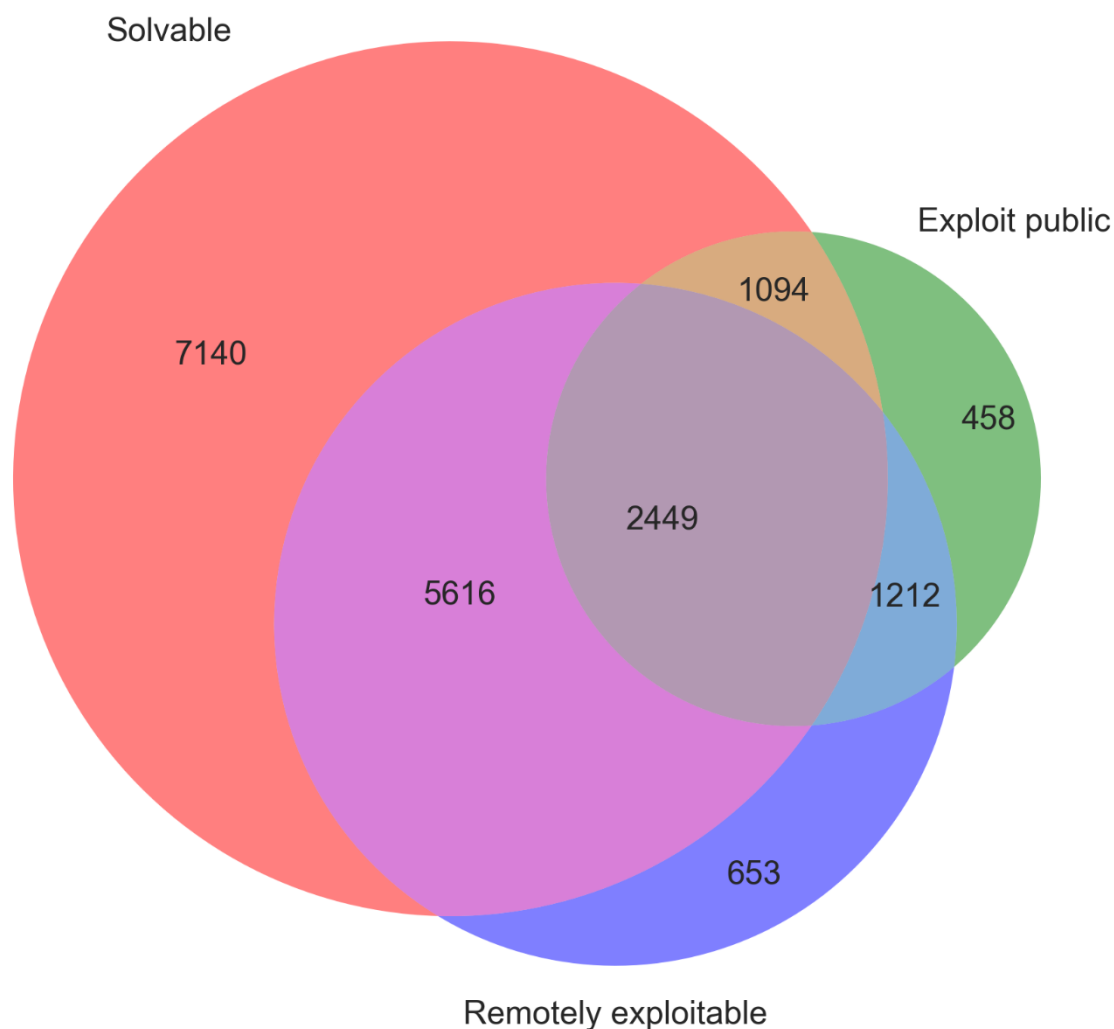


Figure 5, shows that in 2021, CVE / NVD failed to report 8,215 (29%) known disclosed vulnerabilities. In terms of actionability, this number is actually 9,530 (33%) since at the time of writing, 1,315 vulnerabilities are in RESERVED status in CVE. For those unfamiliar with the term, RESERVED status vulnerabilities are entries that have been given CVE IDs, but contain no details in the CVE database. As such, even though these entries are counted towards CVE's total, RESERVED status vulnerabilities are completely unactionable.

**Figure 6:** Breakdown of actionable vulnerabilities, limited to CVE IDs, by availability and ease of exploitation, disclosed by EOY 2021

However, CVE / NVD's inability to detail 33% has a deeper impact on organizations using publicly-sourced data to inform their Vulnerability Management Programs. Looking at figures 4 and 6 side-by-side shows that either CVE severely lacks coverage on remotely exploitable vulnerabilities, or has great difficulty in identifying remote code execution (RCE) entries. Either way, the end result is that security teams planning to use publicly sourced data will be unaware of 60% (1,659) of the vulnerabilities that have all three stipulations, highlighting the importance of having comprehensive, detailed and timely intelligence.

# In Closing

Despite the vulnerability disclosure landscape shaking off the pandemic, there has been no celebratory fanfare. Now, it is back to business-as-usual and that means vulnerability disclosure counts will likely fall back into the pattern of increasing incrementally each year. As such, organizations that still adopt the mindset of “patch everything” will continue to struggle.

The good news is that the industry is starting to make big leaps in how it views vulnerability management. Firms like [Gartner](#) are catching on to the inefficiencies caused by reliance on [vulnerability scanners](#), while government agencies like the Cybersecurity Infrastructure and Security Agency are pushing for organizations to focus their prioritization on metadata like [exploitability](#), rather than severity.

All of these movements are educating organizations that it can be possible to proactively manage risk, rather than always reacting to it. As enterprises take the steps in assessing those possibilities, security teams will come to realize that it will all come down to the quality of data. To make informed risk-decisions, they will come to understand that comprehensive, actionable, and timely vulnerability intelligence will be critical, and that it won't be found in the public source.

## 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 Flashpoint

Trusted by governments and the Fortune 500, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners - including cyber threat intelligence (CTI), vulnerability management, DevSecOps and vendor risk management teams - rely on Flashpoint's intelligence platform to proactively identify and mitigate risk and stay ahead of the evolving threat landscape. To learn more about Flashpoint, visit <https://www.flashpoint-intel.com/> or follow us on Twitter at @FlashpointIntel.

## 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](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 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.