



**RiskBased
SECURITY**

2020 Q3 Report

Vulnerability QuickView



Welcome

This year continues to be a challenge for organizations as the vulnerability disclosure landscape continues to evolve. Earlier in the year we saw a sharp decrease in vulnerability disclosures, yet the drop in disclosed vulnerabilities did not translate to a lessened workload for Vulnerability Managers and IT Security Teams. Instead, what we have seen over the course of the year were multiple [Vulnerability Fujiwhara events](#), when the disclosure schedules of major vendors including Oracle and Microsoft collide, that have hit organizations hard.

Even though the Fujiwhara storm have settled, we are starting to see that “regular” Patch Tuesdays are consistently reaching volumes comparable to January’s event. These events, on top of routine vulnerability disclosures, have steadily closed the gap between the number of vulnerabilities disclosed in 2019 vs 2020, which was -19.2% at the mid-year and stands at -4.6% at the end of Q3, putting us back on track to reach similar numbers as last year.

The 2020 Q3 Vulnerability QuickView Report covers vulnerabilities disclosed between January 1, 2020 and September 30, 2020. We hope that this report helps you navigate the current vulnerability landscape and provides valuable insight into the vulnerability trends we’re seeing in 2020 and how they will affect organizations.

Key Highlights

- Risk Based Security’s VulnDB® team aggregated 17,129 vulnerabilities that were disclosed during the first three quarters of 2020.
- The number of vulnerability disclosures is beginning to return to normal, with 2020 back on track to reach levels similar to those we saw in 2019. In 2020 Q1, when comparing vulnerability disclosures to the same period last year, there was a sharp decrease of 19.2%. Now, in 2020 Q3, that gap has narrowed to 4.6%.
- Risk Based Security has noted 600 vulnerabilities that are still in CVE RESERVED status. Organizations and security products strictly relying on CVE / NVD will find no details in CVE for these entries, despite being public and having a CVE ID associated with them.
- Research suggests that “regular” Patch Tuesdays are reaching volumes comparable to Vulnerability Fujiwhara events. This poses a significant burden for IT security teams and Vulnerability Managers, as resultant remediation efforts can last for weeks.
- Microsoft has seen a 39% increase in reported vulnerabilities for 2020 Q3 compared to last year and has surpassed all other vendors, rising from 9th to 1st on the Top 10 list.

In This Issue

VIEWPOINTS FROM



Brian Martin
Vice President,
Vulnerability Intelligence,
Risk Based Security



Curtis Kang
Cyber Security Content Specialist,
Risk Based Security

WELCOME

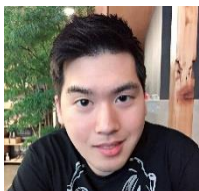
Key Highlights	2
Viewpoints	4
Why EVM Security Hasn't Changed For More Than 15 Years	4
Vulnerability Trends in 2020	9
2020 At A Glance	9
"Top" Products by Confirmed Vulnerabilities	10
"Top" Vendors by Confirmed Vulnerabilities	11
Disclosures Over Time	12
Can CVE Keep Up With Growing Vulnerability Disclosures	13
In Closing	14
About Risk Based Security	15
About VulnDB	15
No Warranty	15

Why EVM Security Hasn't Changed For More Than 15 Years



Brian Martin, Vice President of Vulnerability Intelligence, RBS & Curtis Kang, Cyber Security Content Specialist, RBS

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.



Curtis writes and reports for Risk Based Security. Initially working in the Insurance and Healthcare industries, Curtis was drawn into information security. He holds a bachelor's degree in Marketing with a concentration in Integrated Communications from Virginia Commonwealth University.

In our [2019 Year End Vulnerability QuickView Report](#), we presented a detailed history of public Electronic Voting Machine (EVM) vulnerabilities. We've seen little change to the overall EVM security picture since then. With the [Presidential elections in the U.S.](#) somewhat now in the rear view mirror, it is a good time to take stock of EVM security, and reflect on why so little has changed for the last 16 years.

A HEALTHY AMOUNT OF SKEPTICISM

We're not in the business of speculation, and maybe to your dismay we don't plan to draw conclusions on foreign interference during the November elections.

However, we do plan to continue to shine a spotlight on EVM security (or the lack of it) for several reasons. First, there's been little progress in closing known vulnerabilities in order to better secure the machines. Second, there is no way to audit many vulnerable machines, to even detect if it has been digitally tampered with.

The reality is that EVM security is far from perfect. Yet, despite the obvious concerns we have seen some patterns suggesting that the EVM vendors may not be taking their security duties as seriously as they should.

The Patterns We Have Been Seeing

At Risk Based Security we know it is important to know which of your vendors care about security, and we shine a light on that with our extensive vulnerability and data breach intelligence. Unfortunately, EVM vendors often do not seem particularly willing to embrace transparency, despite the important role that their products play in national security and democracy. Compiling sources and research, there are several key factors that contribute to overall staleness in EVM security.

THE VENDOR MINDSET

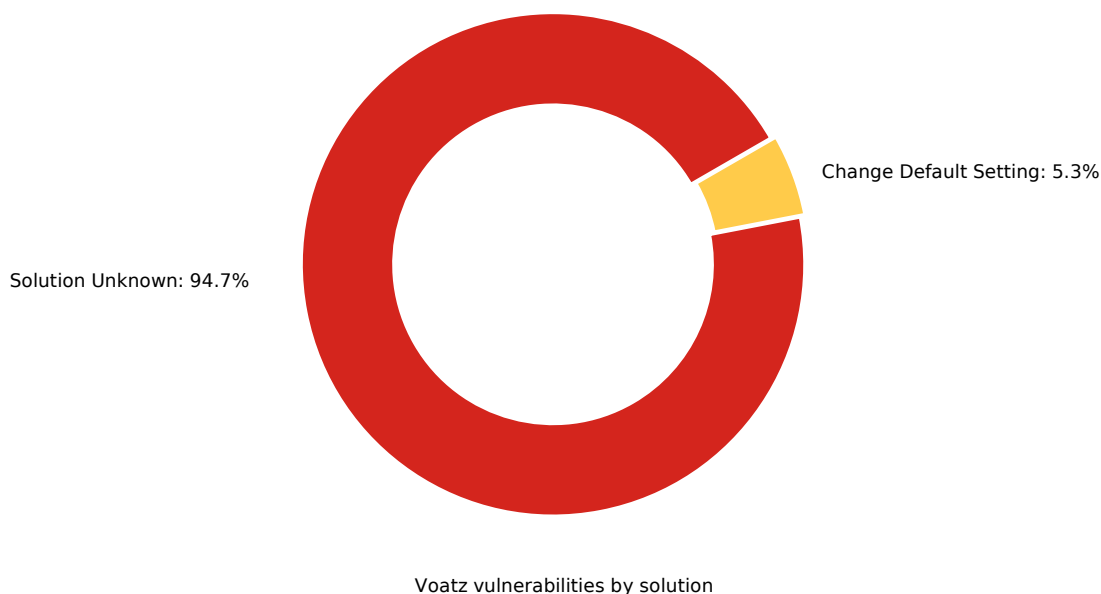
Prior to the election, on January 9th, 2020, witnesses including the CEOs for ES&S, Dominion, and Hart InterCivic testified before the House Administration Committee, telling lawmakers that they had seen no evidence of [election system tampering](#). However, when asked by Rep. Mark Walker of North Carolina to rate themselves between 1-10 on their security practices, each CEO carefully avoided giving a straightforward answer, instead saying that they are doing “*everything they can*.”

But what exactly does that mean? There aren’t many open examples of the measures EVM vendors take in securing these devices, but there are many examples of those vendors doing what they can to limit vulnerability reporting. The recent example of Voatz attempting to influence legislation involving the [Computer Fraud and Abuse Act \(CFAA\)](#) exemplifies the EVM mindset.

To summarize their Amicus Curiae, Voatz favors narrowing the CFAA to restrict independent researchers, stating that they believe open research to be harmful and a waste of tax dollars. Instead, they insist that “*necessary testing and research*” be done only by authorized parties, such as bug bounty programs and private consulting firms.

Voatz, along with many other EVM vendors, are designated as “*critical infrastructure*” by the Department of Homeland Security, so ensuring that these devices are secure should be a no-brainer. Although bug bounty programs play their part, there are concerns within the security community about relying exclusively on this approach. Those within the industry know that corporations using these programs sometimes push [NDAs on participants](#), which can be seen as an attempt to buy a researcher’s silence if they get paid for reporting a vulnerability. Even if a researcher agrees to sign, it doesn’t guarantee that the vulnerability will be fixed by the vendor.

Insistence on limiting who can report a bug can give the impression that vendors are more interested in preventing people from disclosing vulnerabilities in their products than they are in working with researchers to make their products secure. Data within [VulnDB](#) shows that in Voatz’s case, numerous vulnerabilities within their product have been reported since 2013 – in fact one has a CVSS score of 10 *and* is considered to be remotely exploitable. However, despite the considerable passage of time, a solution is still not known.



Another example of the EVM vendor mindset is the official [ES&S Security Test Report](#) produced by Coherent Cyber. Multiple vulnerabilities were found throughout ES&S's main line of products that could allow an attacker to obtain the highest privilege levels, enabling remote access into the system. According to one of the analysts who participated in the report, once ES&S was aware that the evaluation was taking place, they were "appalled" that his team would follow their own testing plan and not ES&S's own preferred plan. Despite Coherent Cyber finding these vulnerabilities, ES&S was unwilling to work with them and informed Coherent Cyber that "they had their own team and were not interested."

But isn't it the duty of a red team to simulate an aggressor? Would an attacker play nice and follow the official testing plan, or would they take advantage of a vulnerable device any way that they could? Malicious attackers have a tendency to disregard safe spaces or play by "the rules."

DOMINATION OF THE MARKET AND FORM OVER FUNCTION

Another key factor is the dominance of the EVM market by a small number of vendors, primarily ES&S, Dominion, and Hart InterCivic. While Coherent Cyber's report should have aroused suspicions regarding the security of the devices provided by these companies, it has not stopped the government from continuing their contracts.

One of the main explanations as to why this is the case comes from the [state's involvement in the voting process](#). The responsibility of conducting and maintaining elections falls upon the states, who then often delegate responsibilities for voting machine selection, vote tabulation, and result validation to specific counties.

As such, counties will purchase machines that are either well-known in the market (like ES&S) or older, "affordable" machines that still function. Most of the time, these affordable machines are nearly ten years old and are from defunct vendors that have been bought out by the above mentioned EVM vendors. They are repackaged, but oftentimes still run on original hardware and software. Coherent Cyber reported that some devices like the [ExpressVote, DS200, and DS850](#) have been found to run on Windows 7, despite Microsoft ending official support on January 14, 2020. News outlets have reported that [these machines](#) were used in the November 2020 U.S. Presidential election.

Many states and counties still rely on these old machines because the emphasis is placed on functionality over security. In fact, the Chairman of the [Election Assistance Commission](#) has arguably gone so far as to advocate the use of older machines:

"Those systems are very old. But they are more like the fact that if you have a classic car, to maintain that classic car, you change the oil, you change the brakes, the tires – that car will continue to function well. What you want to do is make sure that the classic car continues to run well. That is the same thing with voting systems."

-Thomas Hicks, Chairman of the Election Assistance Commission

This analogy is flawed, because it neglects potential security implications. The issue at hand isn't whether these machines will function, the concern is whether a thief can break in. Sure, the brakes and tires may work, but what about the locks? Depending on how old the car is, if someone is looking to break in, they might only need a clothes hanger. In cyber security terms, breaking into old systems is literally child's play [as we saw at Def Con 2018](#).

“STRICT SECURITY PROTOCOLS”

The bottom line is that EVM machines are vulnerable and have many documented, unpatched vulnerabilities. Our own research has revealed that overall, there are 302 documented EVM vulnerabilities and 96% of them do not have a solution available. Unfortunately for the counties responsible for patching and securing these devices, only a single EVM vulnerability has been assigned a CVE ID. When lawmakers are confronted with these and similar findings, they often provide assurances to the public that these systems are “safe” and cite inherent security protocols. However, when these claims are investigated it turns out that the security measures they cite are not sufficient.

In Virginia, the “[worst voting machines](#)” of all time were used between 2003 – 2015 and were riddled with all sorts of problems including **users being able to connect to machines using cellphones**. But when pressured, Virginia officials at the time told voters that the systems were “safe” due to “*strict security protocols*” and continued their use for **seven more years**.

The “*strict security protocols*” cited by these officials turned out to refer to the machine’s Wi-Fi network password. That password was “*abcde*” and was cracked by the FBI in two minutes. The simple existence of a password, despite its inadequacy, was enough to check the box for lawmakers. It has a password? Then it is secure. It’s secure? Then this device is safe. Is the situation any different today? Is it possible that current security concerns are dismissed on similarly weak logic?

Although the specific WINVote machine in this example is discontinued as of right now, it doesn’t change the fact that this insecure device was used for many Virginia elections and the thought process that permitted their continued use may still persist. Machines known to be vulnerable are still in wide circulation across the U.S. and they are being defended by politicians under the same pretenses as the WINVote machines. Sure, these machines may have passwords and “*security protocols*” in place, but that doesn’t mean that they are effective. In the HBO documentary, [Kill Chain: The Cyber War on America’s Elections](#), the security PIN for the TSx machine was revealed to be “11111”, and the pin before that was “111.” Does this sound familiar? These [TSx machines](#) were reported to be used by several counties in 2020 elections. Assurances of security protocols do not make a vulnerable machine secure.

THAT OLD REDUX

We had hoped that the topic of EVM security would be resolved, or at least that substantial progress would have been made before the recent election (and the previous one), but there have been no substantial changes. Despite the discussion being alive for over a decade, we are not very hopeful that it will be fixed anytime soon. To reiterate, Risk Based Security is not saying that the 2016 nor the 2020 elections have been digitally compromised, as there is no evidence showing such and that is outside the scope of this research. What we are saying is that EVM machines have been and continue to remain vulnerable. Given what we know about the past and present, we sincerely hope that real progress can be made to increase transparency with EVM vendors and harden our vital democratic processes.

“Those who cannot remember the past are condemned to repeat it.”

-George Santayana

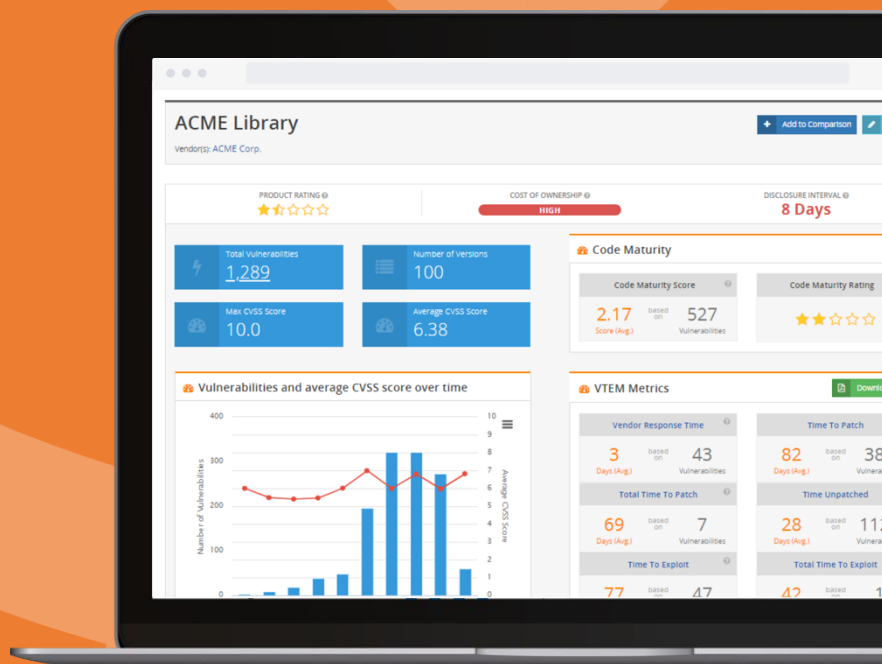
The Vulnerability QuickView report is powered by



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
sales@riskbasedsecurity.com

LEARN MORE

Vulnerability Trends in 2020

2020 At A Glance

At the end of Q1 this year, we saw what appeared to be a sharp decline in vulnerability disclosures as compared to 2019, dropping by 19.2%, from 6,198 to 4,968. Statistically that is huge. But as 2020 continues, we are starting to see just how large an impact the pandemic has had on vulnerability disclosures. Earlier this year we pointed out how COVID-19 was influencing disclosures for a variety of reasons, but we were cautious at making early assumptions. Even though the gap was pretty significant, we hesitated, saying *"this may or may not be a true drop in the number of vulnerabilities."*

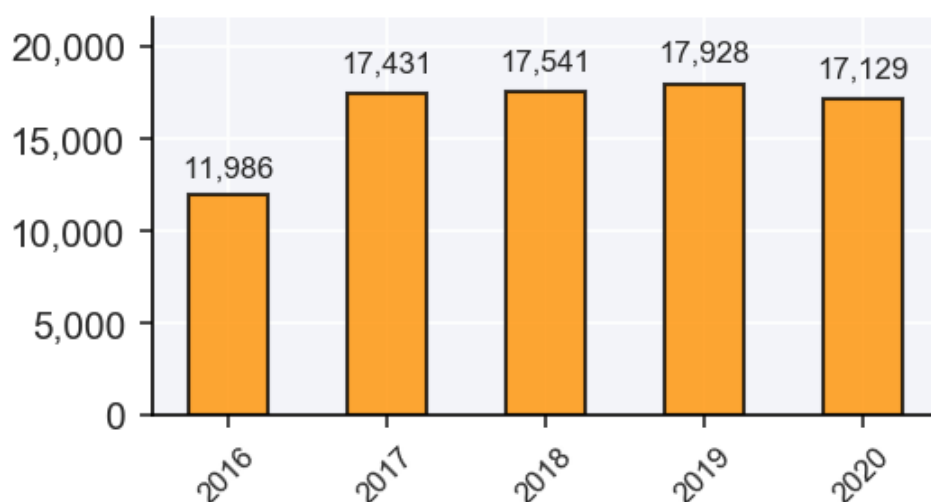


Figure 1: Number of vulnerabilities disclosed by Q3, in the last five years

As the year has progressed the decrease in vulnerabilities being published has begun to return to “normal”. After the mid year point, the gap had dropped to only 8.3% as both researchers and organizations began to resume their old routines. In that report we compared the mid year data from 2019, with 12,118 disclosures, to this year’s, which saw 11,121, and commented that even though it might continue to appear that vulnerability reporting was down, the trend would most likely not continue. That brings us to Q3 where we see that there were 17,928 disclosures by this point in 2019 as compared to 17,129 this year, meaning that the year-over-year gap has narrowed to only 4.6%. That puts us on track to reach vulnerability disclosure totals similar to those of last year as we head into 2021. But with the pandemic seeing a resurgence in most of the world even as we enter the holiday season, it is difficult to predict the exact influence COVID-19 will have on the vulnerability disclosure landscape.

"Top" Products by Confirmed Vulnerabilities

In an effort to answer many people's favorite questions, we can start by looking at "*which product / vendor has the most vulnerabilities?*" Starting with products, we have to give the usual disclaimer that not all operating systems are equivalent for this purpose. Specifically, some will ship with additional software that is not necessarily enabled by default. So, while we may see one operating system have more vulnerabilities than the next, the one with more vulnerabilities may also install "out of box" with fewer that can be exploited.

Compared to last year we see openSUSE remains on top but has dropped considerably in the total number of vulnerabilities. Windows 10 made a significant jump from #15 to #2 and heads up several other Windows distributions, including Windows Server 2019, Windows Server (Semi-Annual Channel), and Windows Server 2016.










Name	Rank 2020	Rank 2019	Count 2020	Count 2019
openSUSE Leap	1	1	820	1189
Windows 10	2 	15	738	501
Windows Server 2019	3 	19	680	464
Debian Linux	4 	2	679	1130
Windows Server (Semi-Annual Channel)	5 	29	665	356
Ubuntu	6 	3	634	969
Red Hat Enterprise Linux for x86_64	7 	5	607	742
Windows Server 2016	8 	27	575	381
Google Pixel / Nexus Devices	9 	25	440	413
Red Hat Enterprise Linux Workstation	10 	14	439	505

Table 1: Top ten products by vulnerability disclosures in the first three quarters of 2020

"Top" Vendors by Confirmed Vulnerabilities

Shifting our focus from products to vendors, we see Microsoft make a significant jump from #9 last year as the end of Q3 to take the top spot now. This is reflected by the corresponding jump in vulnerabilities from 737 to 1202, almost a 39% increase. The second thing that is interesting to point out is that while the vendors jockeyed for position, the same ten vendors appear this year and last year when we look at the year so far, as we can see in the table below.

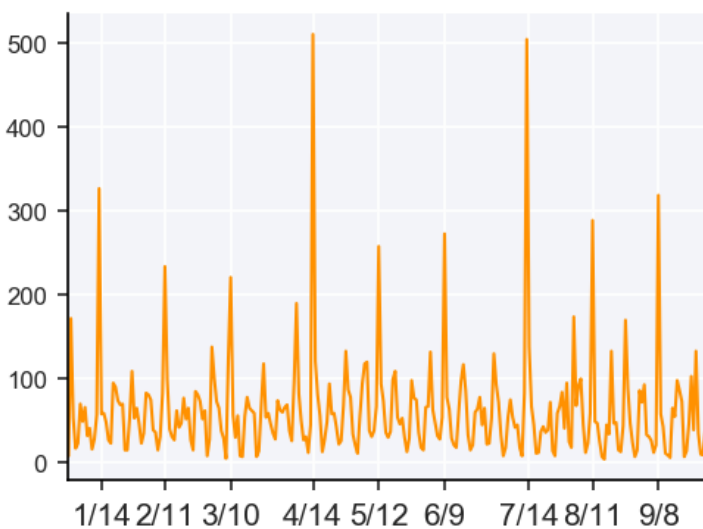
Name	Rank 2020	Rank 2019	Count 2020	Count 2019
Microsoft Corporation	1 ↑	9	1202	737
Oracle Corporation	2	2	1025	1164
Red Hat	3 ↑	6	961	1015
Google	4 ↑	7	905	995
SUSE	5 ↓	1	901	1288
IBM Corporation	6 ↓	4	817	1086
Software in the Public Interest, Inc.	7 ↓	3	680	1131
Canonical Ltd.	8	8	635	971
Cisco Systems	9 ↑	10	558	499
Dell	10 ↓	5	504	1079

Table 2: Top ten vendors by vulnerability disclosures in the first three quarters of 2020

Disclosures Over Time

With three Vulnerability Fujiwhara events behind us this year, two in particular stand out when looking at the disclosures over time this year. April 14 (511 disclosures) and July 14 (496 disclosures) were both huge events in the world of vulnerability management as Oracle released a quarterly Critical Patch Updates (CPU) on the same day that Microsoft and other vendors that have adopted the 'Patch Tuesday' schedule disclosed vulnerabilities in their products. Fortunately for administrators, 2020 was an anomaly and the next Fujiwhara event won't come for another five years.

The first 2020 Fujiwhara event, in January, was not as significant. In fact, the volume of disclosures was about the same as that of September's Patch Tuesday despite the major vendors all contributing to the total. This illustrates how even "regular" Patch Tuesdays have grown to be serious undertakings that represent an incredible burden on IT teams, with remediation efforts that can last weeks. That can often give IT teams just a few days each month before the grind starts again.



Three significant peaks in 2020 Q3:

- April 7th with 190 vulnerabilities
- August 3rd with 174 vulnerabilities
- August 25th with 170 vulnerabilities

Figure 2: Number of disclosures each month in the first three quarters of 2020

Also of interest in the disclosure timeline are three specific smaller spikes; April 7th which reached 190 vulnerabilities, August 3rd with 174, and August 25th with 170. These spikes show that even some "normal" days are outliers and represent a significant jump in disclosures over the daily average of 68.

Can CVE Keep Up With Growing Vulnerability Disclosures?

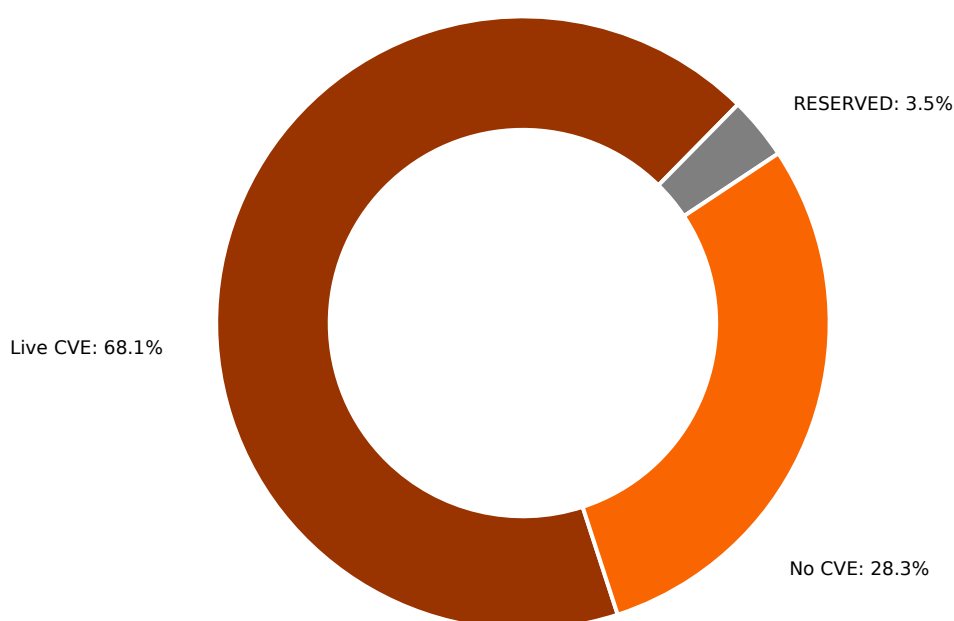


Figure 4: Breakdown of vulnerabilities compared to CVE in the first three quarters of 2020

Examining the vulnerabilities disclosed through 2020 Q3, it is eye-opening to look at a breakdown of CVE coverage. As our loyal readers know, we're quick to point out the lack of coverage offered by CVE / NVD. In this case we see almost **a third** of vulnerabilities disclosed so far in 2020 have not yet been addressed by CVE but can be found in VulnDB. More specifically, of that third, 3.5% of those Q3 entries that do have CVE IDs are still in RESERVED status. That means that organizations relying on stock CVE data, or on products based on CVE / NVD, will find no details in CVE for these vulnerabilities, even though they are public and **do** have a CVE ID associated with them.

While that represents "only" 600 vulnerabilities, it clearly illustrates a difference in approaches to vulnerability aggregation. MITRE's approach with CVE is to wait for researchers and vendors to come to them with details, at their discretion. Using a substantially different approach, Risk Based Security is proactive by monitoring thousands of sources on a nearly continuous basis looking for vulnerability disclosures. By doing this we are able to offer broad coverage of recognized disclosure points, while allowing us to steadily locate new sources to monitor. The chart above illustrates the results of that difference.

In Closing

Although COVID-19 continues to have an unpredictable effect, vulnerability disclosures are currently on track to reach or surpass the levels we saw last year. In our last report we stated that this year's Vulnerability Fujiwhara had a significant part in the increase of vulnerability disclosures. At the time of that report, the Vulnerability Fujiwhara events were solely responsible for 7.3% of all vulnerabilities. But since mid year 2020, the gap in vulnerability reporting vs 2019 has decreased from 8.2% to 4.6%. Unfortunately for organizations, the gap continues to steadily close due to the increasing volume of regular Patch Tuesday events.

It goes without saying that as Patch Tuesday workloads increase, the time needed for remediation will follow suit. But for organizations who are still relying solely on CVE / NVD, they may find that their timeline may be further extended as the number of vulnerabilities "missed" by MITRE remains consistent. As we saw with the issue of [Electronic Voting Machine \(EVM\)](#) security, actions need to be taken to fix the systemic issues or we will continue to see the same problems year after year. Enlightened organizations who are willing to break free of the cycle may want to consider improving their vulnerability management programs by relying on VulnDB - the most comprehensive and timely intelligence solution available.

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.

CVE: Mission vs. Expectations

One of the fundamental objectives of VulnDB is to expand our search methods and collect as many vulnerabilities as possible, to provide our clients with the most comprehensive vulnerability intelligence available, allowing them to determine which vulnerabilities are important to their organization.

While we maintain a curated list of thousands of sources that are monitored on an hourly, daily, and weekly basis, new sources are discovered and/or are brought to our attention every day. CVE on the other hand, issues CVE IDs when requested by a vendor or researcher. Their mission is not to search for vulnerabilities like a vulnerability intelligence company. Rather, they are charged with assigning IDs and keeping minimal records.

Why then do organizations, scanning companies, risk platforms, and security service providers continue to use CVE / NDV as a vulnerability intelligence service and continue to insist that it is "good enough"? Who is best served by this approach? Certainly not those organizations, government agencies and consumers victimized by the increasing number of data breaches from exploited software vulnerabilities.

About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Vulnerability Intelligence, Vendor Risk Ratings, and Data Breaches. Our products, Cyber Risk Analytics (CRA), VulnDB and YourCISO, provide organizations access to the most comprehensive threat intelligence knowledge bases available, including advanced search capabilities, access to raw data via API, and email alerting to assist organizations in taking the right actions in a timely manner.

For more information, visit 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

LEARN MORE

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.