FLASHPOINT

The State of Vulnerability Intelligence

2022 Midyear Edition

In This Issue

Welcome

to the State of Vulnerability Intelligence

Security teams are under great pressure. They are expected to remediate tens of thousands of vulnerabilities each year with limited resources. But with new issues being disclosed everyday, in addition to a major shift to focusing on exploitable vulnerabilities and Advanced Persistent Threats (APT) attacks, organizations are struggling to make workloads manageable.

The only way to effectively remediate risk is by adopting a risk-based vulnerability management program, and that is only possible using quality vulnerability intelligence. The **State of Vulnerability Intelligence: 2022 Midyear Edition** demonstrates the importance of understanding the full intelligence picture, showcasing how better data leads to better risk decisions.

Insights from the report are derived from VulnDB®, the most comprehensive and timely source of vulnerability intelligence available. We hope that this report—which covers vulnerabilities disclosed between January 1 to June 30—helps your organization gain a clear and actionable picture of the vulnerability landscape.

Key Findings

- Flashpoint collected 11,860 vulnerabilities in the first six months of the year, with CVE / NVD failing to report and detail 27.3 percent of them.
- Organizations need to be aware that the vulnerability disclosure landscape is highly volatile, with "standard" days potentially introducing volumes traditionally seen only on Patch Tuesdays and other similar events.
- Vulnerability Management Programs using CVSSv2 scores as a basis for prioritization may be misguided, as Flashpoint has found that 52 percent of all 10.0 vulnerabilities reported in 2022 H1 are likely scored incorrectly.
- Flashpoint has observed a discrepancy of 85 percent concerning “discovered-in-the-wild” vulnerabilities reported in 2022 H1, compared to resources such as Google’s Project Zero showing that exploitation more often occurs outside of Advanced Persistent Threat (APT) attacks.
- Security teams can maximize resources and reduce their immediate workload by 82 percent by first focusing on actionable, high severity vulnerabilities.

Total Known Vulnerabilities

2022 Midyear vulnerability trends

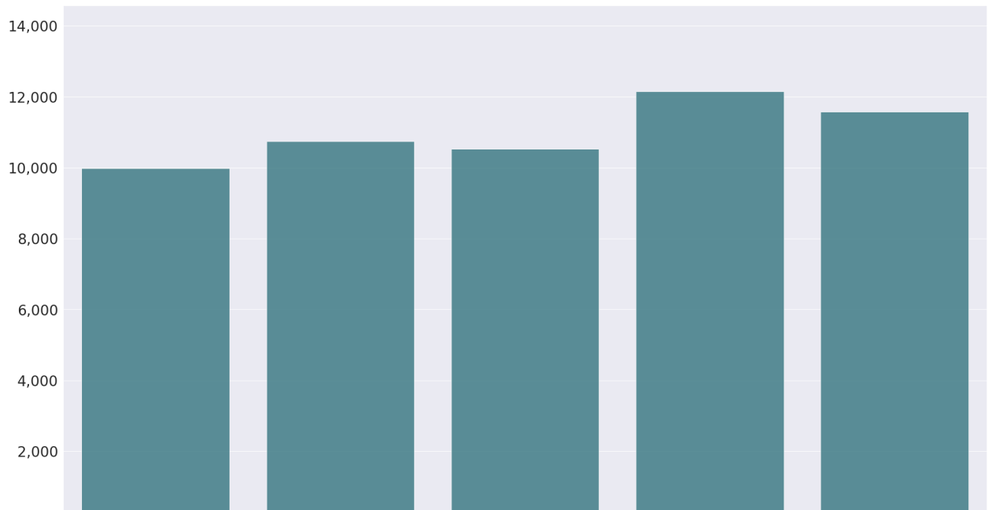

Figure 1: Number of vulnerabilities disclosed by H1, in the last five years

The first half of 2022 saw fewer disclosures (11,860) than 2021 (12,160) based on the chart above. But as we have frequently noted in past reports, as time progresses, the numbers are likely to increase due to backfilling. Backfilling is a process where our research team adds previously reported disclosures as we discover new sources of vulnerability intelligence, ultimately benefitting our customers. This will likely increase 2022’s numbers by the end of year, putting its totals above last year. We should see more disclosures in due time.

Disclosures Over Time

2022 Midyear vulnerability trends

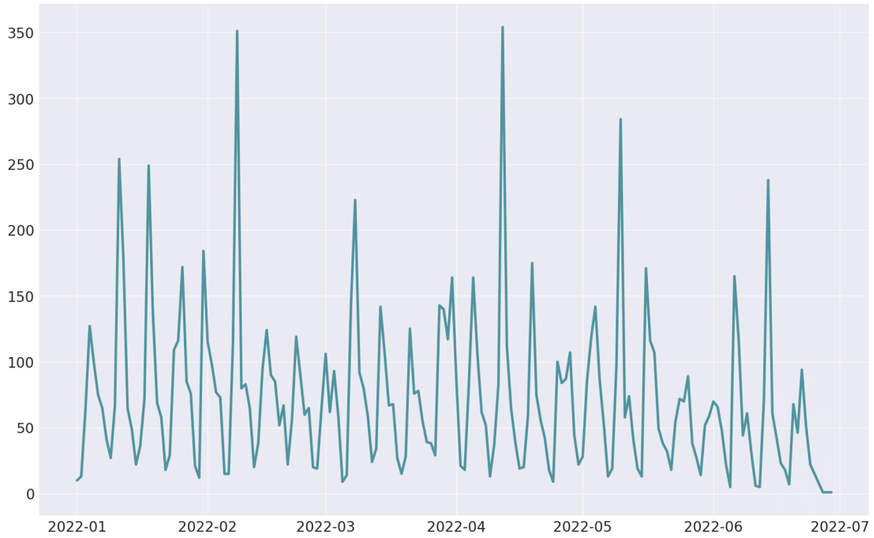

Figure 2: Vulnerability disclosures each day in 2022, up to end of H1

Figure 2 shows the total number of vulnerability disclosures reported, per day, within the 2022 midyear period. Immediately, several large spikes stand out. On average, about 90 vulnerabilities were disclosed per day this year, but January was the worst month for security teams, having four days with above average disclosure volumes—totaling 868. Two of those instances were predictable and security teams had advanced notice: Patch Tuesday and the quarterly Oracle CPU. However, on the other two days, notable vendors such as Cisco, Juniper, and Bentley unexpectedly disclosed multiple vulnerabilities. Organizations need to be aware that the vulnerability disclosure landscape is highly volatile, with "standard" days potentially introducing volumes traditionally seen only on Patch Tuesdays and other similar events.

The following are the dates, events, and totals associated with the largest spikes observed in the 2022 midyear period:

Date	Number of Vulnerabilities	Event / Vendor Release
2022-01-11	255	Patch Tuesday
2022-01-12	180	Cisco (25), Juniper (31) + other vendors
2022-01-18	248	Oracle Quarterly CPU
2022-01-31	185	Bentley (95) + standard disclosure
2022-02-08	351	Patch Tuesday
2022-03-08	224	Patch Tuesday
2022-04-12	356	Patch Tuesday
2022-04-19	180	Oracle Quarterly CPU
2022-05-10	284	Patch Tuesday
2022-06-14	246	Patch Tuesday

Table 1: Dates in 2022 H1 that had the most vulnerability disclosures, attributed by event or vendor release

Top Products and Vendors by Known Vulnerabilities

2022 Midyear vulnerability trends

Name	2022 Count	2021 Count	2022 Rank	2021 Rank
Debian Linux	712	727	1	2
openSUSE Leap	610	779	2	1
Ubuntu	538	607	3	4
SuSE Linux Enterprise Server (SLES)	468	419	4	9
SUSE Linux Enterprise High Performance Computing	450	380	5	12
SUSE Manager Server	447	322	6	19
SUSE Manager Proxy	441	322	7	20
SUSE Linux Enterprise Server for SAP Applications	420	63	8	20+
SUSE Manager Retail Branch Server	386	299	9	20+
SUSE Linux Enterprise Server for SAP	373	374	10	14

Table 2: Top ten products by vulnerability disclosures reported by 2022 H1, as compared to 2021

Name	2022 Count	2021 Count	2022 Rank	2021 Rank
SUSE	735	856	1	2
Software in the Public Interest, Inc.	712	727	2	4
Microsoft Corporation	677	650	3	9
Google	573	651	4	8
Canonical	538	609	5	10
Oracle Corporation	526	817	6	3
Dell	510	725	7	5
Red Hat	493	707	8	6
IBM Corporation	414	934	9	1
XEROX CORPORATION	288	397	10	13

Table 3: Top ten vendors by vulnerability disclosures reported by 2022 H1, as compared to 2021

Organizations tend to be interested in which products and vendors have the most known vulnerabilities. However, it is important that business leaders do not interpret vulnerability totals as a positive or negative indicator of a vendor's security posture: this data should not be the basis for product comparisons or assessments.

There are many underlying reasons as to why certain products and vendors tend to have high vulnerability counts, such as overall market share, product-specific market share, routine (or lack of) schedule of disclosures, attention from vulnerability researchers, and vendor response/patch time, among others. Therefore, organizations should not be immediately concerned about well-known vendors having "more" vulnerabilities, as it could be a sign that they are actively disclosing and patching issues.

Additionally, teams should consider the severity of issues (this doesn't mean a base CVSS score always tells the whole picture), as 100 high-access complexity low-risk issues are not as impactful as 10 remote code execution vulnerabilities are.

Instead, business leaders looking to understand cost of ownership or the overall security posture of deployed vendors should use vulnerability disclosure dates, exploit publication dates, and solution publication dates—a collection of proprietary metadata that Flashpoint calls Vulnerability Timeline and Exposure Metrics (VTEM). Knowing how fast a vendor responds to vulnerability reports is considerably more meaningful than how many total vulnerabilities are present.

> "It is important that business leaders do not interpret vulnerability totals as a positive or negative indicator of a **vendor's security posture**."

The Value of Metadata

Examining the intelligence gap

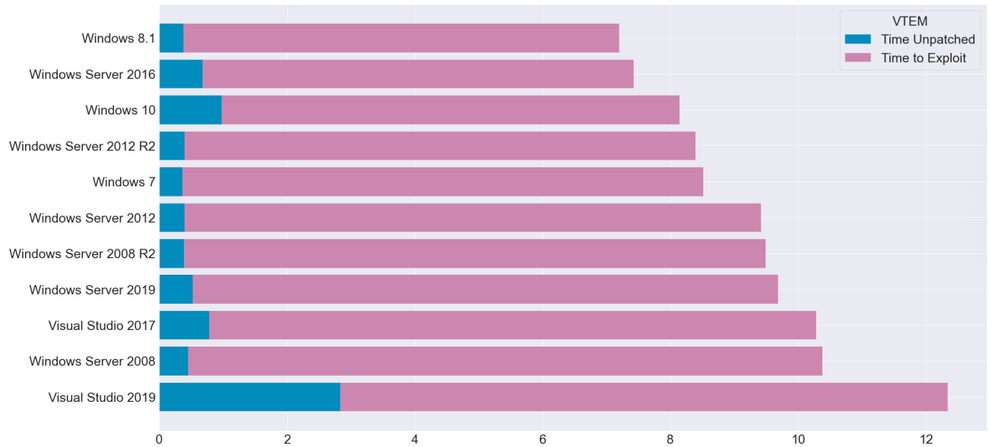

Figure 3: Vulnerability Timeline and Exposure Metrics (VTEM) for Microsoft Corporation

Figure 3 uses VTEM data to demonstrate how long, on average, it takes for a vendor, in this case, Microsoft, to patch vulnerable products before an exploit is available. Comparing the chart above to Microsoft's third spot in Table 3 provides much needed context, while also revealing deeper insights.

For example, it took Microsoft a significant amount of time to release a patch for the zero-day vulnerability dubbed Follina (CVE-2022-30157). However, on average, Microsoft is usually very responsive in releasing solutions for their products. Therefore, even with Follina accounted for, all products affected by that vulnerability are still patched faster than industry norms.

Having this level of metadata helps security teams better understand their environment, potentially identifying weak-spots that outside vendors can introduce, enabling business leaders to make informed risk decisions.

Name	2022 Count	2021 Count	2022 Rank	2021 Rank
SUSE	735	856	1	2
Software in the Public Interest, Inc.	712	727	2	4
Microsoft Corporation	**677**	**650**	**3**	**9**
Google	573	651	4	8
Canonical	538	609	5	10
Oracle Corporation	526	817	6	3
Dell	510	725	7	5
Red Hat	493	707	8	6
IBM Corporation	414	934	9	1
XEROX CORPORATION	288	397	10	13

Table 3: Top ten vendors by vulnerability disclosures reported by 2022 H1, as compared to 2021

www.flashpoint.io

© Copyright 2022 Flashpoint. All Rights Reserved.

FLASHPOINT

VulnDB® and CVE / NVD

Examining the intelligence gap

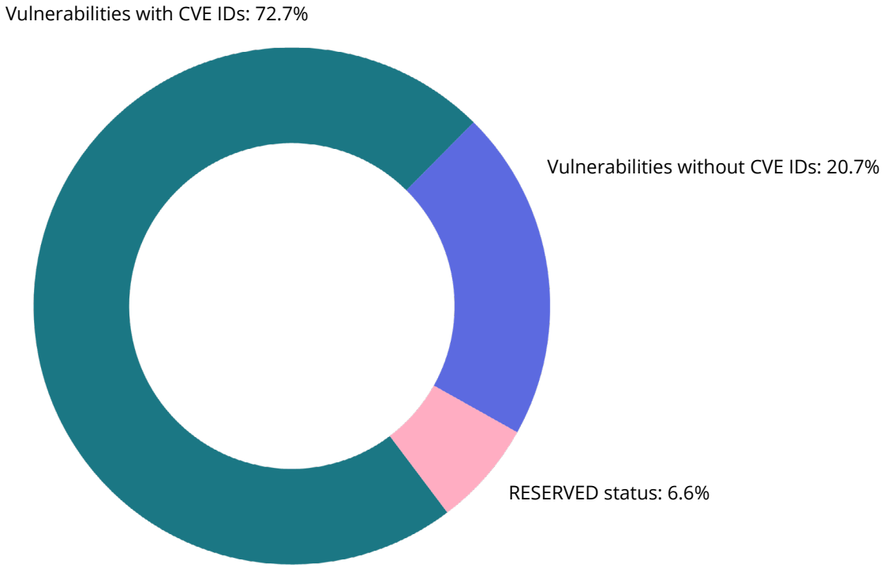

Figure 4: Breakdown of vulnerabilities compared to CVE in 2022 H1

To make better risk decisions, you need comprehensive vulnerability intelligence. Comparing Flashpoint's VulnDB® coverage to MITRE and NIST, CVE / NVD failed to report 20.7 percent of all known disclosed vulnerabilities in the first half of 2022. However, although the public source was unaware of those issues, the actual coverage delta was actually 27.3 percent due to CVE's high number of RESERVED status vulnerabilities—which are vulnerabilities that are given CVE IDs, but have no details in the respective databases.

Business leaders need to be aware that these issues are not trivial, as by nature, all zero-days would start in RESERVED status if they hypothetically had an ID from the start. Also, highly exploitable and high-profile vulnerabilities often start in RESERVED status. For example, CVE-2022-26485 and CVE-2022-26486 were added to CISA's Known Exploited Vulnerabilities Catalog on March 7, 2022. Solution information for these vulnerabilities have been released as well as other valuable metadata, but at time of writing, both of these issues are still in RESERVED status, despite having a remediation due date of March 21.

This highlights that organizations cannot wait for vulnerabilities to be included and updated in CVE / NVD, as they often remain in that state for indeterminate periods of time. And while some may eventually be given proper analysis, this does not always happen. Despite CVE / NVD being seen as a definitive source of vulnerability intelligence, organizations need to know that the public source is, and has been, incomplete since its inception. Looking at the full intelligence picture, strict reliance on CVE / NVD data will result in a risk aperture of over 94,000 vulnerabilities.

> "To make better risk decisions, you need comprehensive vulnerability intelligence. Comparing Flashpoint's VulnDB coverage to MITRE and NIST, **CVE / NVD failed to report and detail 27.3 percent** of all known disclosed vulnerabilities in the first half of 2022."

Potential Issues Caused by CVSS scoring

Examining the intelligence gap

CVSS scores are calculated formulaically, using the following metrics: Access Vector, Access Complexity, and the vulnerability's impact on authentication, confidentiality, integrity, and availability. However, when scoring, CVSS guidelines dictate to "score for the worst" if details involving any of those are unclear.

This practice is intended to ensure that vulnerabilities are not scored too low, which can cause security teams to focus on other issues that are deemed to be more critical in terms of CVSS. This has resulted in many vulnerabilities being scored a 10.0, even though they are actually less severe, due to vendors providing fewer details. Flashpoint's VulnDB® team classifies these vulnerabilities as "unspecified."

Date	Number of unspecified 10.0 vulnerabilities reported by H1	Percent of total 10.0 vulns reported by H1 (rounded)
2022	363	52% (697)
2021	475	60% (793)
2020	509	52% (971)
2019	517	59% (875)
2018	631	65% (977)
2017	440	55% (803)
2016	415	42% (980)
2015	332	43% (771)
2014	300	46% (657)
2013	278	43% (641)
2012	163	50% (323)

Table 4: Number of "unspecified" 10.0 vulnerabilities compared to known total of CVSSv2 rated 10.0

So how does this impact vulnerability prioritization? Looking at the past 10 years, in the same midyear period, we see that on average, 51.5 percent of all known 10.0 scored vulnerabilities are unspecified. This means organizations could be prioritizing hundreds of issues that may not actually be 10.0—further highlighting that base CVSS scores alone should not drive vulnerability management processes.

Discovered-in-the-wild

Examining the intelligence gap

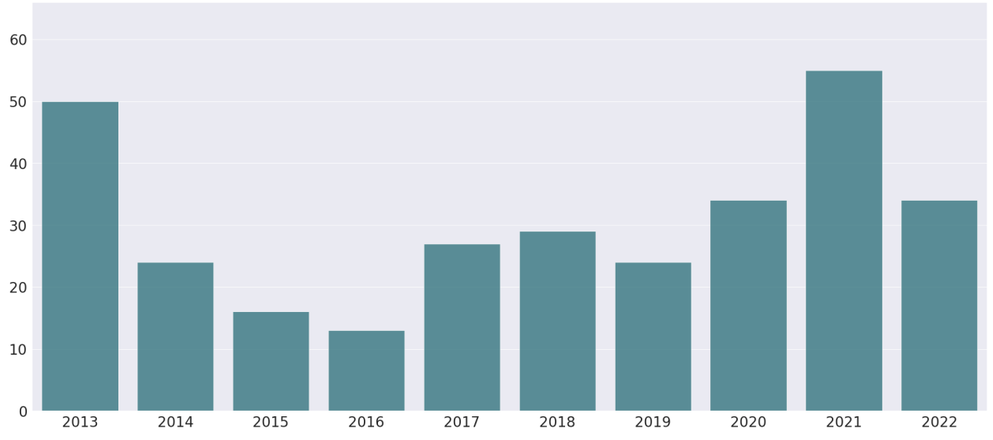

Figure 5: Number of discovered-in-the-wild vulnerabilities collected by H1, in the last ten years

"Discovered-in-the-wild" is a classification given to vulnerabilities that were found to be actively exploited by malicious parties before public disclosure. Each vulnerability classified this way represents an organization being compromised via a vulnerability they had no knowledge of.

Discovered-in-the-wild vulnerabilities are often used in high-profile breaches or are attributed to Advanced Persistent Threat (APT) attacks. Due to their nature, organizations often lack defensive options for them. However, business leaders need to keep in mind that discovered-in-the-wild vulnerabilities represent a tiny fraction of compromises occurring around the world.

Projects like Google's Project0 are great resources for concerned organizations. However, security programs that allocate resources for monitoring discovered-in-the-wild vulnerabilities should be aware that resources often do not list every issue with this classification. Caveats such as project scope often prevents them from doing so. In terms of VulnDB® coverage, we believe it is necessary that we try to collect every vulnerability and let our stakeholders determine what is important to them.

In 2022 H1, Flashpoint aggregated 37 discovered-in-the-wild vulnerabilities, compared to Project Zero's 20. But examining all known discovered-in-the-wild vulnerabilities, Flashpoint's research teams collected 311 vulnerabilities with this classification—versus Project Zero tracking 221. These statements are not meant to downplay Project Zero's effectiveness or efforts. Instead, it shows that there are vulnerabilities within this classification that fall outside of Project Zero's scope. And although they have not been observed to be used by APTs in their attacks, having knowledge of these issues can greatly benefit private sector organizations as they affect commonly-used software and developing technologies such as the blockchain. Ultimately, it communicates that an organization was exploited by a malicious third-party, regardless of being designated an APT or not.

For organizations looking to best protect themselves against zero-day vulnerabilities, it is critical that they maintain a good security posture and be diligent on security procedures—implementing both human and technical security controls. Network segregation, access controls, responsive patching, and user awareness should be a cornerstone of their security program.

"Although some discovered-in-the-wild vulnerabilities have not been observed to be used by APTs in their attacks, having knowledge of them can greatly benefit private sector organizations as they affect commonly used software and developing technologies such as **the blockchain.**"

Importance of Actionable, High Severity

Examining the intelligence gap

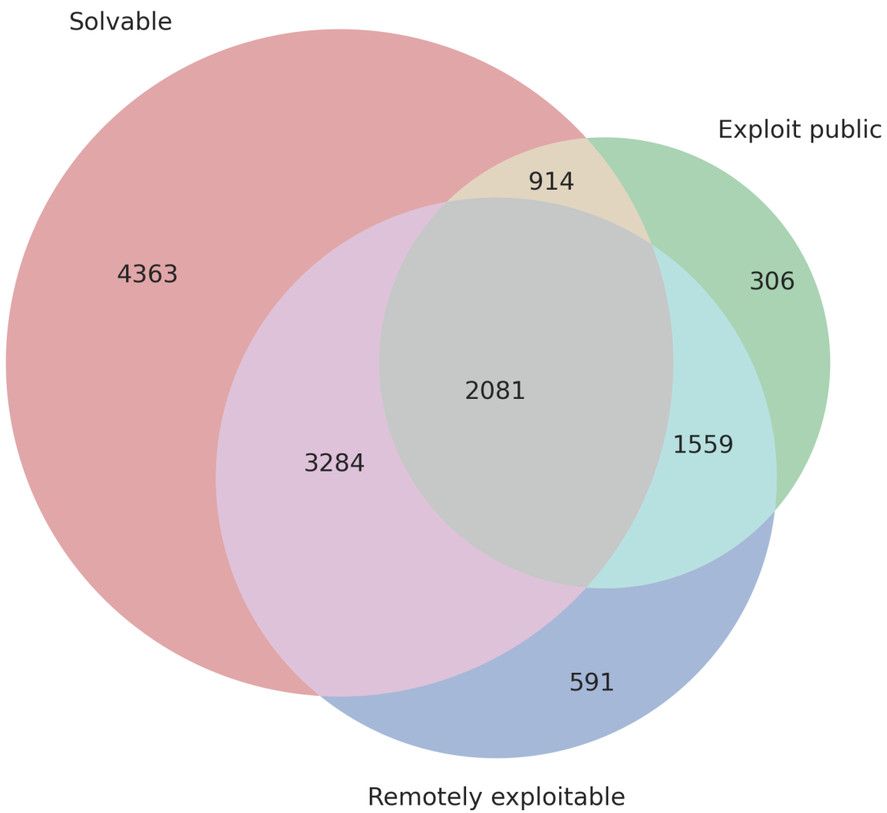

Figure 6: Breakdown of actionable, high severity vulnerabilities, by availability and ease of exploitation, disclosed by 2022 H1

Actionable, high severity vulnerabilities should guide prioritization, as it allows organizations to maximize resources while providing the best results. Vulnerabilities that are considered to be in the actionable, high severity category have all three characteristics: they are remotely exploitable, have a public exploit, in addition to having a viable solution, like a patch or upgrade. For this midyear period, 2,081 vulnerabilities hit this 'sweet spot'.

These vulnerabilities should be at the top of the list for triaging, as they pose the most risk, yet are the quickest to remediate. Security teams can reduce their immediate workload by 82 percent, by focusing on actionable, high severity vulnerabilities. Once those issues are addressed, security teams can then examine the remainder, using a risk-based approach that prioritizes at-risk assets based on business need, rather than uncontextualized base CVSS scores. As such, using these three points of metadata can be incredibly helpful for security teams to quickly reduce the most risk in their environment, resulting in better outcomes compared to top-down patching. Simple queries against a complete data set gives more power and flexibility for your team,

> “Security teams can **reduce their immediate workload by 82 percent**, by focusing on actionable, high severity vulnerabilities.”

www.flashpoint.io

© Copyright 2022 Flashpoint. All Rights Reserved.

Conclusion

Security teams are struggling with incredible workloads, and their backlog of tasks constantly grows as Patch Tuesdays, Oracle CPUs, and the almost daily ongoing activity from CISA continues to be released. And while organizations understand the importance of triaging all of these issues, as well as being proactive overall, they can only do so with well curated data.

As this report has shown again, CVE / NVD data remains incomplete. Publicly available data is uncontextualized and often misses valuable metadata which ultimately can misguide your teams' prioritization and remediation processes. In addition, **CVE / NVD has failed to report 27.3 percent of vulnerabilities known to VulnDB® within the period outlined by this report**. However, important details for those unreported issues exist and can be found within VulnDB®. If organizations seek better risk decisions, they need the full intelligence picture so that they can adopt a risk-based approach that best fits their needs.

Methodology and terms

VulnDB® vulnerability intelligence is derived from a proprietary methodology and daily analysis of thousands of vulnerability sources. Unlike some vulnerability database providers, Flashpoint Intelligence 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.

Detect and remediate vulnerabilities faster with Flashpoint

Having a comprehensive source of vulnerability intelligence is essential to ensuring that risk is remediated in a timely manner. Sign up for a **free VulnDB trial** to gain visibility into the vulnerabilities that the public source misses while also experiencing full, detailed coverage of CVE / NVD.

Credits

Thank you to Brian Martin, Ben Haynes, and Curtis Kang for their contributions, along with the entire Flashpoint Intelligence Team, for your tireless research and analysis, which make reports like these possible.

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.

FLASHPOINT To learn more, visit **flashpoint.io**