

# Vulnerability Intelligence Report



# Contents

---

**Summary** 03

Key Takeaways 04

---

**Introduction** 05

---

**The State of Vulnerabilities** 06

Vulnerability Disclosure Trends 06

Key Takeaways 06

Analysis 07

CVSS Versions and Prioritization 09

**Top Vulnerabilities** 11

Key Takeaways 12

Analysis 13

Top 20 Vulnerabilities Chart 16

Conclusions 19

Web Browser and  
Application Vulnerabilities 20

Key Takeaways 20

Web Browser Vulnerabilities 21

Top 10 Web Browser Vulnerabilities Chart 23

Application Vulnerabilities 26

Top 10 Application Vulnerabilities Chart 30

---

**High-Profile Vulnerabilities** 32

Vulnerability Timeline 33

---

**Contributors** 36

Primary Research 36

Subject Matter Experts 36

---

**Appendix** 37

CVSS Severity Ratings 37

CVE Disclosure Years 37

**Methodology** 38

Data Set 38

Prevalence 38

CVEs Versus Vulnerabilities 38

Interview Methodology 38

---

**Endnotes** 39

# Summary

In this report, we provide an overview of current vulnerability disclosure trends and insights into real-world vulnerability demographics in enterprise environments. We analyze vulnerability prevalence in the wild, based on the number of affected enterprises, to highlight vulnerabilities that security practitioners are dealing with in practice – not just in theory. Our study confirms that managing vulnerabilities is a challenge of scale, velocity and volume. It is not just an engineering challenge, but requires a risk-centric view to prioritize thousands of vulnerabilities that superficially all seem the same.

Throughout this report, we use the terms “vulnerability” and “CVE” interchangeably. Common Vulnerabilities and Exposures<sup>1</sup> (CVE) is “a list of entries – each containing an identification number, a description and at least one public reference – for publicly known cybersecurity vulnerabilities.”<sup>2</sup> A CVE identifier describes a unique vulnerability, whereby “unique” can refer to unique on a given operating system for a specific version rather than in general.

In reality, multiple CVEs can refer to the same “vulnerability” (e.g., a vulnerability affecting a browser available on multiple operating systems such as Microsoft Windows, Red Hat Enterprise Linux and SUSE Linux).

To ensure that we have comparable data for new and old vulnerabilities, whenever we refer to “CVSS” or “severity,” we are generally referring to CVSSv2, unless we state otherwise. We generally use CVSSv2 when comparing historical vulnerability data and CVSSv3 only when considering more recent ones, where CVSSv3 data is available.

# Key Takeaways

## The growth in new vulnerabilities continues unabated:

- 15,038 new vulnerabilities were published in 2017 to CVE<sup>3</sup> versus 9,837 in 2016, an increase of **53%**.
- The first half of 2018 shows an increase of **27%** versus the first half of 2017. We are on track for 18,000–19,000 new vulnerabilities this year.

## Prioritizing based on High severity or exploitability alone is becoming increasingly ineffective due to the sheer volume:

- **54%** of new CVEs in 2017 were rated as CVSSv3 7.0 (High) or higher.
- Public exploits are available for **7%** of vulnerabilities.
- For vulnerabilities where both CVSS version 2 and 3 scores are available and a comparison is possible (mainly post-2016), CVSSv3 scores the majority of vulnerabilities as High or Critical (CVSSv2 **31%** versus CVSSv3 **60%**).

## Enterprise vulnerability management is a challenge of scale, volume and velocity:

- The live population (22,625) of distinct vulnerabilities that actually resides in enterprise environments represents **23%** of all possible CVEs (107,710).
- Almost two-thirds (**61%**) of the vulnerabilities that enterprises find in their environments have a CVSSv2 severity of High (7.0–10.0).
- Vulnerabilities with a CVSSv2 score of 9.0–10.0 represent **12%** of the entire vulnerability population. On average, an enterprise finds 870 CVEs per day across 960 assets<sup>4</sup>. This means that prioritization methodologies based on remediating only Critical CVEs still leave the average enterprise with more than a hundred vulnerabilities per day to prioritize per patch, often on multiple systems.
- Considerable amounts of old Oracle Java, Adobe Flash and Microsoft IE and Office vulnerabilities were discovered in enterprise environments (some older than a decade). Old, discontinued and end-of-life applications are out there – and legacy applications are still a major source of residual risk.

# Introduction

The discovery and disclosure of vulnerabilities continue to grow in volume and pace. In 2017 alone, an average of 41 new vulnerabilities were published every single day, for a total of 15,038 for the year. Additionally, the growth in newly disclosed vulnerabilities from the first half of 2018 showed a 27 percent increase over the first half of 2017.<sup>5</sup>

High-profile vulnerabilities have also become a regular feature in mainstream headlines and are often cited as the root cause of massive data breaches. Whether the Equifax breach<sup>6</sup> or WannaCry<sup>7</sup>, the reality is many high-profile incidents could have been prevented through better cyber hygiene. In fact, 57 percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause<sup>8</sup>.

Zero-days and advanced threats are compelling topics for the media, but advanced threats – especially nation-state threat actors – are not an everyday occurrence for the average enterprise. The majority of data breaches do not involve sophisticated attacks or zero-day exploits.

It's true that if you can defend yourself against advanced threats, you will also be able to stop opportunistic attacks. But, the converse is not. If you can't stop basic threats, you will definitely fail to defend against more advanced ones. More importantly, even though we will never realistically be able to mitigate every vulnerability that exists in our environments, we can present a hardened surface to make an attacker's life as difficult as possible.

At the same time, we also have to be realistic and recognize that maintaining good cyber hygiene is difficult. It requires cross-organizational and multi-domain collaboration and orchestration. Business units must try to reconcile conflicting objectives and priorities for the sake of reducing risk. The truth is, the technical complexities and challenges of scale involved in managing enterprise vulnerabilities are rarely the only inhibitor to developing and running a mature vulnerability management program. Effective threat and vulnerability management also depends on the harmony between people, processes and technology.

Aside from social engineering as the initial attack vector, the majority of modern breaches are a direct consequence

of ineffective vulnerability management. Our own research bears this out. In our [“Quantifying the Attacker’s First-Mover Advantage”<sup>9</sup> report from May 2018](#), we discovered that attackers have a seven-day window where an exploit is available before enterprises even become aware they are vulnerable. In our [“Cyber Defender Strategies”<sup>10</sup> report](#), we found almost 52 percent of enterprises have a low maturity when it comes to vulnerability assessment.

Trying to remediate and mitigate all disclosed vulnerabilities, even when prioritizing High and Critical vulnerabilities, is an exercise in futility, as our data shows. The reality is, for most vulnerabilities, a working exploit is never developed. And, of those, an even smaller subset is actively weaponized and employed by threat actors.

Managing vulnerabilities at volume and scale across different teams requires actionable intelligence. Otherwise, we're not making informed decisions – we're guessing. An intelligence deficit in vulnerability management is causing real-world implications – with 34 percent of breached organizations stating they were aware of the vulnerability that led to their breach before it happened.<sup>11</sup>

The problem is we have too much information and not enough intelligence. Turning information into intelligence requires interpretation and analysis – something that doesn't scale easily. The solution lies in operationalizing intelligence based on your organization's unique characteristics – your most critical digital assets and vulnerabilities.

This report presents a bit of both – general overall trends in vulnerabilities and operationalized intelligence based on what enterprises actually have to deal with in their own environments.

This report also introduces the Top 20 Vulnerabilities Chart, providing insight into the most prevalent vulnerabilities across different technologies in enterprise environments. The Top 20 Vulnerabilities Chart harnesses real-world telemetry data to determine which vulnerabilities are really present in enterprise environments, rather than just existing in vulnerability databases, thus providing a more reliable window into the true state of the vulnerability population.

# The State of Vulnerabilities

## Vulnerability Disclosure Trends

In this section, we look at current vulnerability disclosure trends. To denote specific vulnerabilities, we use Common Vulnerability and Exposures (CVE) IDs. CVE itself has some known issues, especially around comprehensiveness and timeliness,<sup>12</sup> but it is considered an official standard by many and we use it here as a baseline.

### KEY TAKEAWAYS

#### The growth in newly disclosed vulnerabilities continues unabated in 2017:

- 15,038 new vulnerabilities were disclosed versus 9,837 in 2016 – an increase of **53%**.
- For **7%** of all disclosed vulnerabilities, public exploits were available.
- **54%** of new CVEs in 2017 were rated as CVSSv3 7.0 (High) or higher.
- Between 18,000 to 19,000 new vulnerabilities are projected for 2018, with a current growth rate of **27%** compared to 2017.

#### The shift from CVSSv2 to CVSSv3 has a huge impact on the distribution of severity:

- CVSSv3 scores the majority of vulnerabilities as High and Critical.
- CVSSv2 scores **31%** of CVEs as High severity, versus **60%** with High or Critical severity under CVSSv3.

As a prioritization metric at volume and scale, CVSS lacks sufficient granularity to differentiate between degrees of criticality.

# ANALYSIS

## Counting Vulnerabilities and the NVD Backlog

Many studies base the publication date of a CVE on the publication date on the National Vulnerability Database (NVD)<sup>13</sup>. For example, a CVE-2017 vulnerability that wasn't published to NVD until 2018 would be classed as a 2018 vulnerability.

The issue with this methodology is the well-known backlog<sup>14</sup> in new vulnerabilities being added to NVD. Many vulnerabilities are publicly disclosed in the year corresponding to their CVE ID, not their NVD publication date. For example, CVE-2017-1000391 is listed on NVD with a publication date of January 25, 2018,<sup>15</sup> even though the advisory was released on November 8, 2017.<sup>16</sup>

There are edge cases where a vulnerability was, for example, assigned a CVE in 2016 but not disclosed publicly until 2018. However, more commonly, a vendor assigns a CVE and publishes an advisory, but there is a delay until it is processed by NVD.

Our methodology is to count all CVE-2017 vulnerabilities in the 2017 data set. Except for the edge cases mentioned above, this more accurately reflects the number of vulnerabilities that customers actually have to manage.

The chart below (Figure 1) compares the "official" count of CVEs on an annual basis since 2010 to the reality. The average annual backlog is around 13 percent.

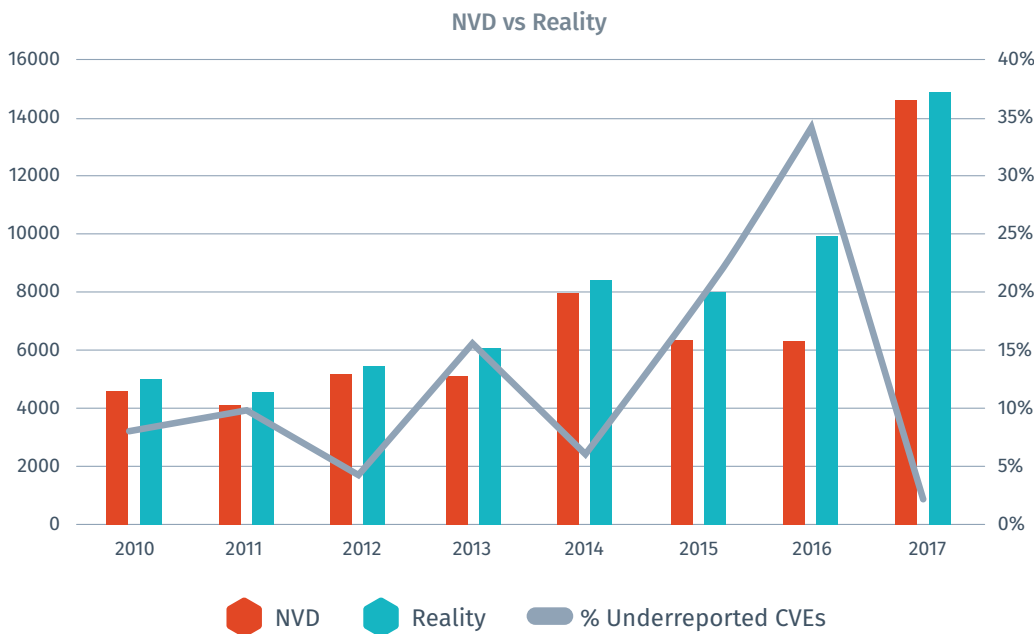


Figure 1. CVEs published to NVD vs CVEs actually publicly disclosed

## Vulnerability Publication Trends

In 2017, 15,038 CVEs were disclosed – a growth of 53 percent compared to 2016. Average year-over-year growth since 2010 has been 15 percent. And, the growth in disclosed vulnerabilities and published CVEs proceeds unabated in 2018.

In the first half of 2018, 5,314 CVEs were published, compared to 4,189 in the first half of 2017 – an increase of 27 percent. At the current pace, we are on track for 18,000 to 19,000 new vulnerabilities in 2018. See summary in Figure 2.

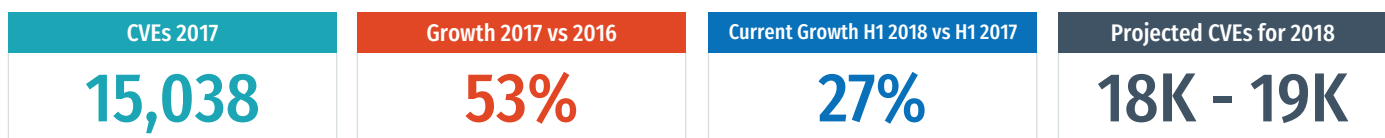


Figure 2. Growth in published CVEs 2010–2017, including projection for 2018

### Disclosed CVEs & Exploitability

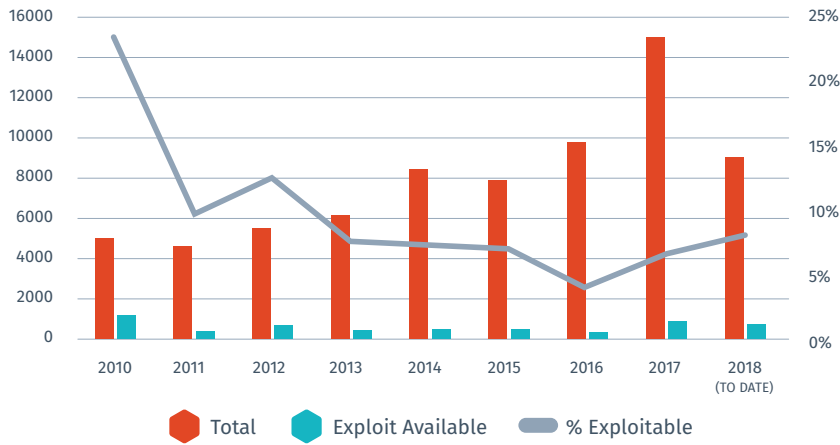


Figure 3. Total CVEs vs. exploitable CVEs

### Exploitability

Meanwhile, the proportion of CVEs with a publicly available exploit is projected to reach eight percent in 2018, down two percentage points from 2017. At current projections, more than 1,500 exploitable vulnerabilities will be published in 2018 – just over 28 exploitable vulnerabilities every week.

### Vulnerability Severity Trends

Very few CVSSv3 scores are available for vulnerabilities prior to 2016, so our historical analyses focuses on CVSSv2. What is noticeable in the chart to the right (Figure 4) is that while there is a corresponding increase of High severity vulnerabilities (CVSSv2 7.0 and higher), these vulnerabilities have actually been in decline as a proportion of the total since 2017. In theory, that still potentially left more than 3,900 High severity vulnerabilities to prioritize. (Note: The 2018 data is not complete and is based on disclosed CVEs through August 2018.)

### New CVEs Severity 'High' and Above 2010-2018

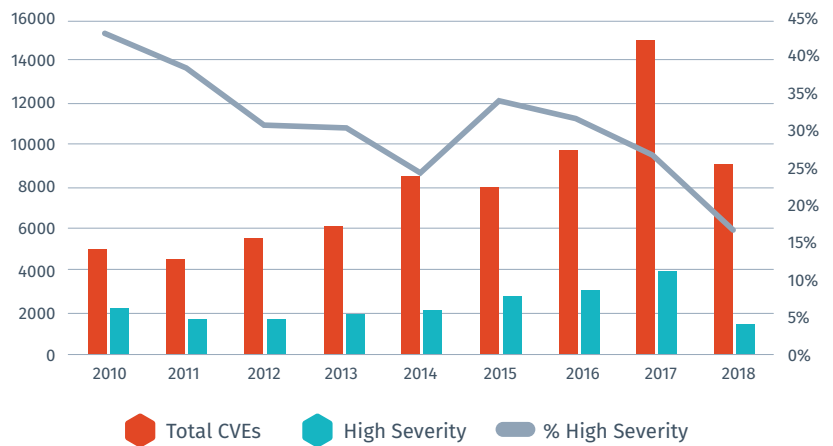


Figure 4. New CVEs 2010-2018

For newer vulnerabilities, we can directly compare the CVSSv2 versus CVSSv3 distribution. One thing to note is that CVSSv3 designates a severity of Critical for scores from 9.0 to 10.0 whereas CVSSv2 assigns any score from 7.0 to 10.0 a High severity.

When we compare the distribution of CVSSv3 severities between the first half of 2017 and the first half of 2018, we see that Critical severity vulnerabilities constituted 15 percent of all disclosed vulnerabilities, up from 12 percent in the first half of 2017. If the current trend continues, we will see more than 900 Critical severity vulnerabilities by the end of 2018.

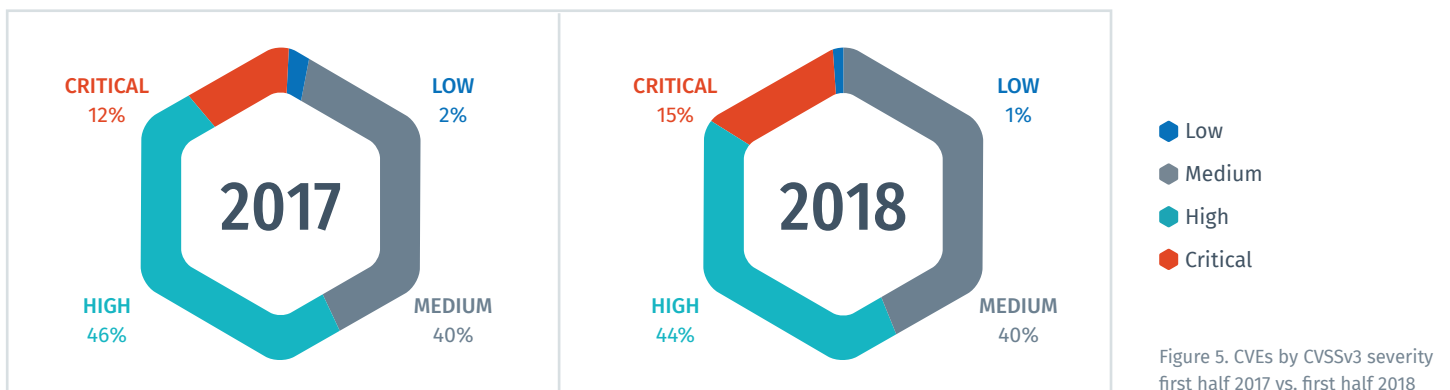


Figure 5. CVEs by CVSSv3 severity first half 2017 vs. first half 2018



## CVSS VERSIONS AND PRIORITIZATION

CVSSv3 was released in June 2015 and is intended to supersede CVSSv2. CVSSv3 included several changes mainly relating to scope. For example, CVSSv3 doesn't just consider how a vulnerability affects the original vulnerable component, but also whether the vulnerability affects other components on the system (e.g., a vulnerability in a web server could also affect connected web browsers). Cross-site scripting and SQL injection vulnerabilities are good examples.

Another change is the level of user interaction required for successful exploitation is now a standalone metric –

not just a factor in the complexity metric. Additionally, an official Critical severity was added to the existing severities of Low, Medium and High.

For most vulnerabilities prior to 2016, a CVSSv3 score is not available, but we can draw comparisons for newer CVEs. When we compare the CVSSv2 and the CVSSv3 severity distribution for all CVEs that have both scores available, there is a visible shift to the right toward a higher severity. Many CVEs considered Medium under CVSSv2 are reclassified as High or Critical under CVSSv3 (see Figure 6).

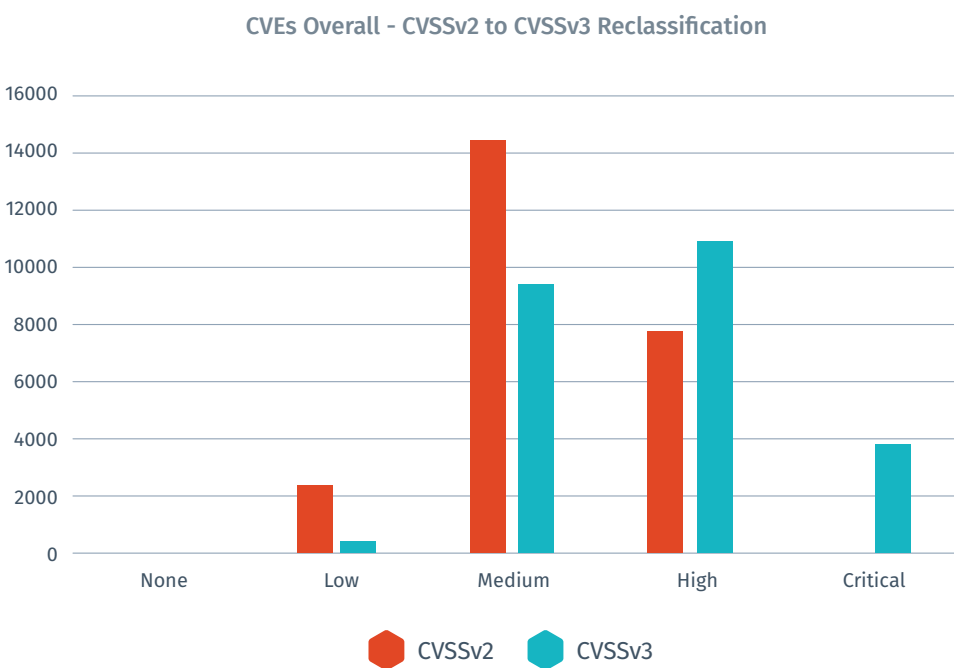


Figure 6. CVEs overall – CVSSv2 vs. CVSSv3 classification

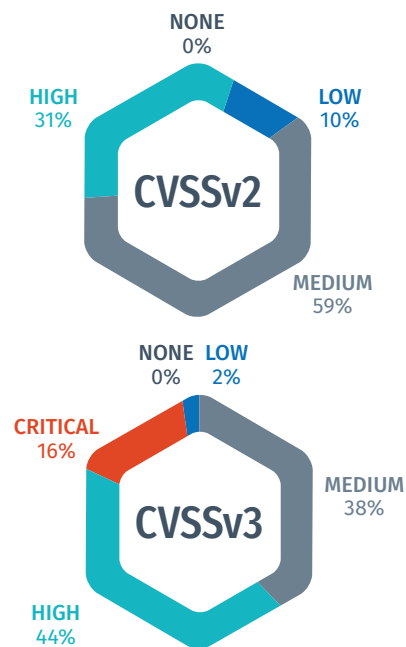


Figure 7. CVEs overall – CVSS severity distributions

So, why do we see this shift? One reason is that under CVSSv2, the impact assessment focuses on the impact to the operating system. But, under CVSSv3, the impact considers the vulnerable component and other affected components and assesses whichever one is most severe. Another change that likely caused this shift was the removal of Medium attack complexity, which results in many vulnerabilities shifting down to a Low attack complexity.

The shift from CVSSv2 to CVSSv3 has a huge impact on the distribution of CVE severities. The two systems provide conflicting ratings, and CVSSv3 scores the majority of vulnerabilities as High and Critical (60 percent in CVSSv3 versus 31 percent in CVSSv2). As a prioritization metric, CVSS is woefully inadequate – lacking sufficient granularity and broader perspective to differentiate between degrees of criticality.

## Insights from the Field

To add real-world perspective to the data, Tenable Research conducted interviews with security practitioners at both the manager and analyst level about vulnerability management strategy and practice. Key insights from these interviews are included throughout this report.

“ I think there was an increase of 14% compared to last year. We’re talking about 200,000 vulnerabilities or something.

Because interviewees practice vulnerability management daily, they didn’t talk much about the volume of vulnerabilities they face today. For them, mitigating vulnerabilities is a given.

“ There’s no destination to vulnerability management. This is a journey. It will always be a thing. And if you ever stopped doing it, you’re gonna open yourself up to a massive amount of risk. So it’s...just a process really [...] You can’t put a project around it. I mean, you can do an implementation project, but you will never be done with vulnerabilities. You can’t put an end date on it.

Instead, these security professionals reflected on the work required to segment and prioritize vulnerabilities in a useful way. Due to the sheer volume of vulnerabilities being disclosed and the nature of CVSS scores, most participants developed some form of custom scoring to prioritize vulnerabilities on their organizations’ systems.

“ The CVSS scores would be useful if you assume that all the assets were equal, which they’re not. So, we don’t really use it.

Generally, they struggled to think of new trends in vulnerabilities for 2018. Some even reflected on 2018 being a relatively standard year compared to previous ones.

“ After last year, there’s not a whole lot that’ll surprise me. That was a rough year, you know, between WannaCry, NotPetya, all the ransomware and all that stuff going on. So, this year, thankfully, has been pretty quiet for the most part. 2017 will always be the year I compare for now, at least. I’m sure another year will come up.

One interviewee commented that researchers and attackers might be “going deeper” in looking for vulnerabilities.

“ They’re looking into new areas where people haven’t looked before. So, they’re finding a lot that has lived for a long time because no one is looking there. Spectre and Meltdown are examples of that. And I think we will see similar things coming up in the future [...] People are running out of cross-site scripting to find and are starting to look in other places.

One vulnerability trend a few participants pointed out was cryptocurrency mining operations, specifically ones exploiting vulnerabilities in Oracle WebLogic.

“ Cryptomining, I think, is taking over the the attack trends and some of it very rapidly. So, we noticed it at the end of last year. And it was coming in through two vectors. One of the vectors was surprisingly WebLogic [...] Historically, it’s not something that was high on our list when we did our scanning.

# Top Vulnerabilities

A disclosed vulnerability is really just a description. CVE itself is a good example, being a dictionary of common names (i.e., CVE Identifiers) for publicly known vulnerabilities. The NVD, in turn, is a database that documents the actual details pertaining to a vulnerability using the CVEs as unique identifiers.

If we want to draw an analogy, the CVE and NVD details are similar to describing a new disease. They tell you: what the disease is called, what it looks like, how it infects or “exploits” a host and about its symptoms. But, they tell you nothing about how many people are potentially vulnerable to, or affected by, the disease.

So, while analyzing overall trends about new and historical vulnerabilities is useful to gain an understanding of how vulnerabilities themselves are evolving, you must look to real-world telemetry data to really understand which vulnerabilities are actually present in enterprise environments – subsequently representing the greatest true risk.

We analyzed the vulnerability prevalence data from March to August 2018 across a data set containing more than 900,000 unique vulnerability assessments conducted by 2,100 individual enterprises from 66 countries to determine the most prevalent vulnerabilities.

To measure prevalence, we looked at the highest one-day peak of affected enterprises (i.e., enterprises where the vulnerability was detected in a vulnerability assessment scan [see Appendix for further details]). We also used the highest one-day peak for affected assets as a secondary metric.

## KEY TAKEAWAYS

The live population of vulnerabilities that actually resides in enterprise environments represents **23%** of all possible CVEs.

Almost two-thirds (**61%**) of the vulnerabilities that enterprises find in their environments have a High severity (CVSSv2 7.0–10.0).

Vulnerabilities with a CVSSv2 score of 9.0–10.0 represent **12%** of the entire vulnerability population. On average, an enterprise finds 870 CVEs per day across 960 assets.<sup>17</sup> This means that prioritization methodologies based on remediating only these High (or critical) CVEs still leave the average enterprise with more than a hundred vulnerabilities per day to prioritize per patch, often on multiple systems.

We clearly see a difference between local risk and global risk:

- Some vendors, like Linux distributions such as Red Hat, Oracle and Novell SUSE, rank high in the amount of distinct CVEs present in the wild, but their impact in terms of affected organizations or assets is low. These represent a local risk – high and important to the affected organization, but not necessarily to the greater global internet population.
- Other vendors, such as Microsoft (.NET and Office), Adobe (Flash) and Oracle (Java), have a comparatively low amount of distinct vulnerabilities, but affect a large amount of enterprises and assets. These represent a global risk, as they affect a large number of enterprises and assets worldwide.

Microsoft and Adobe Flash vulnerabilities feature most prominently in the top 20 vulnerabilities based on the percentage of affected enterprises. (See Top 20 Vulnerabilities Chart.)

**27%** of enterprises still detected services using insecure SSLv2 and SSLv3 versions.

# ANALYSIS

In total, there were 24,625 distinct CVEs from Low to High severity in the data set. 107,710 CVEs have been published as of October 2018, so the live population of vulnerabilities in enterprise environments represents 23% of all possible CVEs.

The distribution of severity across the data set can be seen in the chart below (see Figure 8). The chart shows the count and distributions of unique CVEs detected across enterprise environments from March through August 2018.

Distinct CVEs by Vendor and Severity

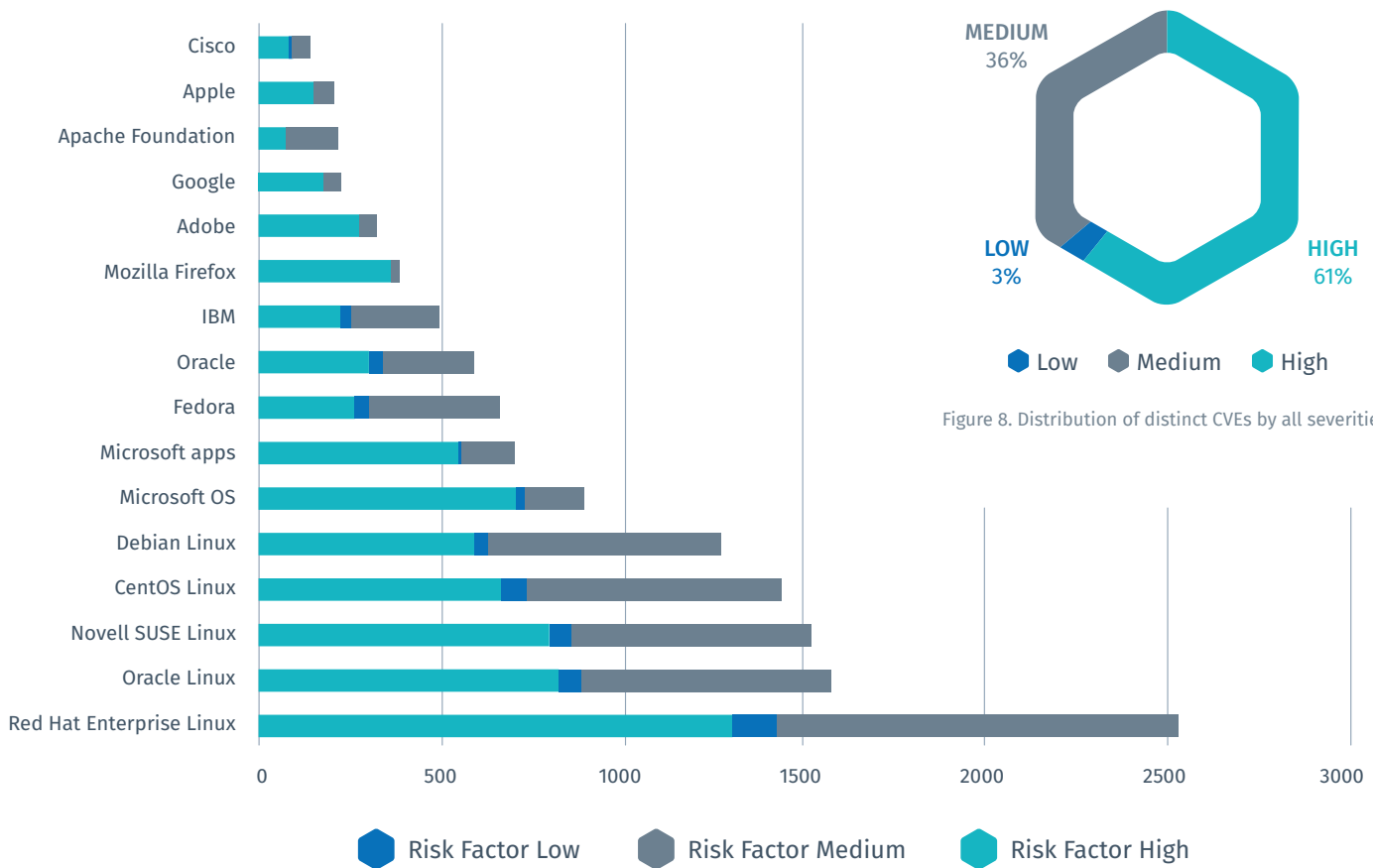


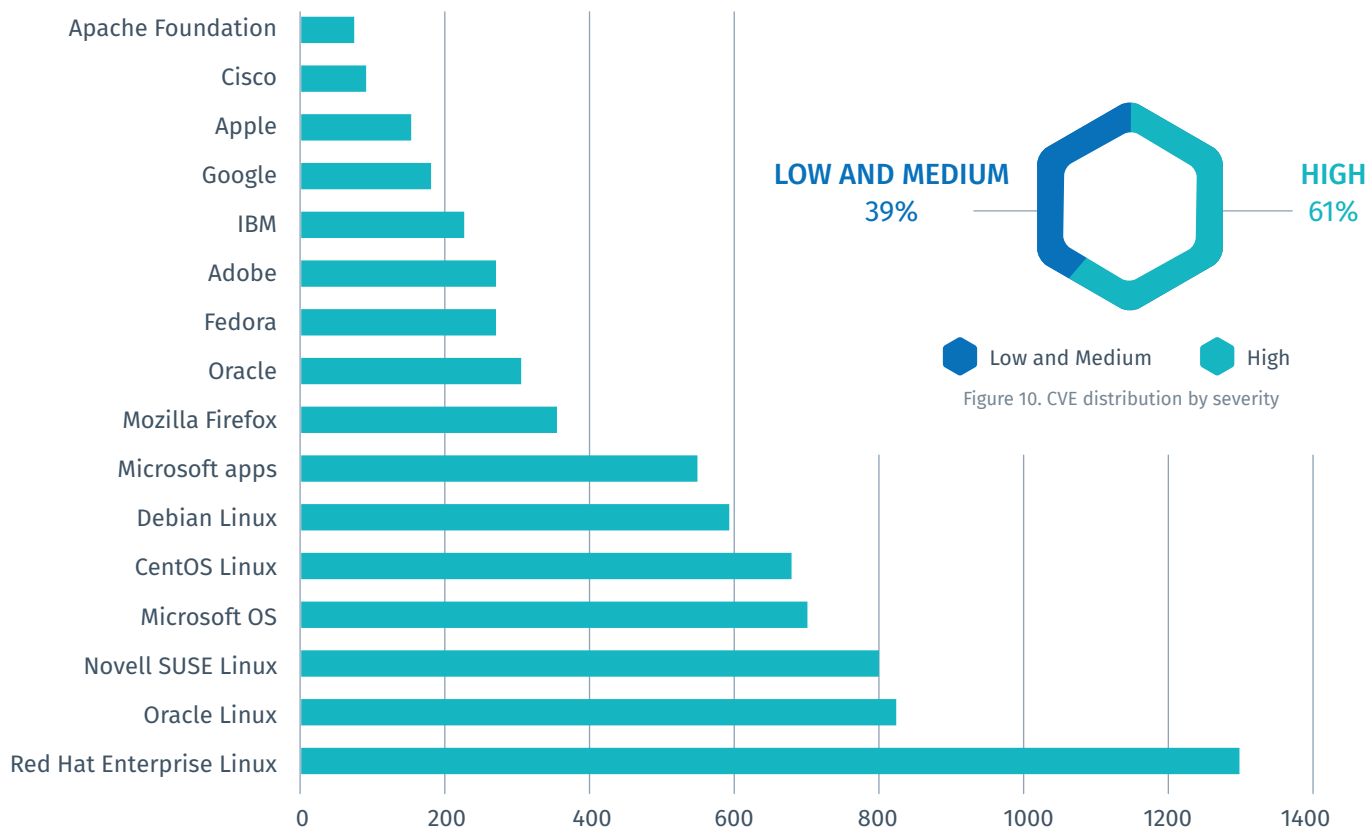
Figure 8. Distribution of distinct CVEs by all severities

Figure 9. Distinct CVEs by vendor and all severities

The amount of distinct CVEs detected for Red Hat Enterprise Linux is by far the highest, with Linux distributions generally dominating the upper rankings. At first glance, this may indicate that Linux is generally less secure. But, we need to consider that for Linux distributions, the core OS and third-party application vulnerabilities are aggregated. If we wanted a comparable view for Microsoft Windows, we would need to consider the Microsoft applications and Microsoft OS groupings in aggregate. We also would need to consider that this data only looks at the count of distinct detected vulnerabilities – not the count of affected assets or enterprises.

Also noticeable is that 61 percent of the CVEs were rated with a CVSSv2 High severity.

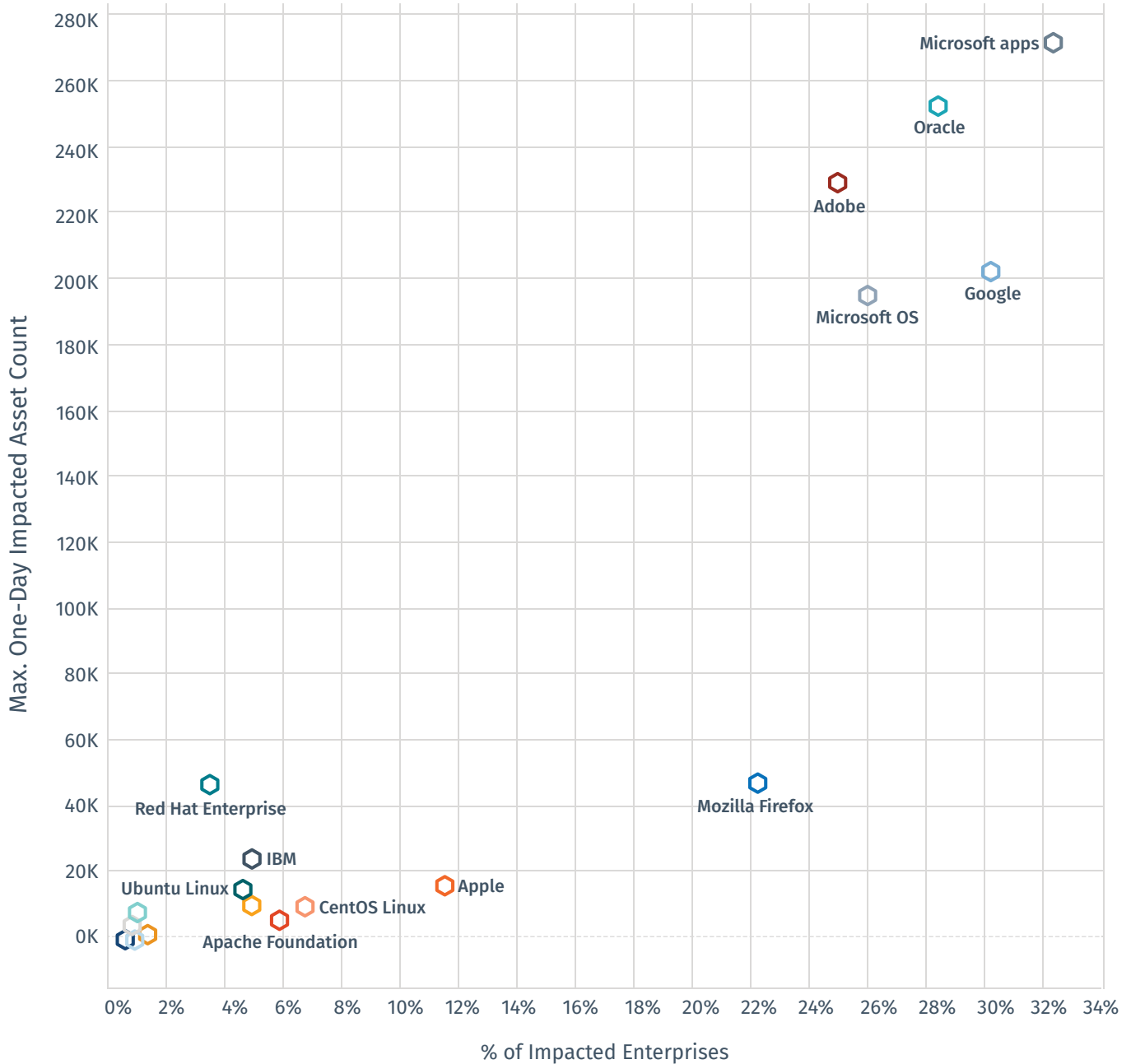
### Distinct CVEs by Vendor - High Severity



The analyses above focus on the count of distinct CVEs and their distribution by vendor. This provides some insight into the vulnerability – and resulting risk profile – of different vendors. It also highlights how prioritization can be more challenging when dealing with some technologies versus others. To see how much risk a given CVE represents in the overall enterprise population, we must look at how many enterprises are actually affected by a given CVE. The chart below (see Figure 12) shows the maximum number of affected enterprises and assets on a single scan day for the same vendors we highlighted above. It clearly shows that a high count of vulnerabilities (e.g., in Red Hat or SUSE Linux) does not necessarily equate to a high count of affected enterprises or assets.

A high count of distinct High severity vulnerabilities on a single or a few assets represents a high local risk. A low count of distinct High severity vulnerabilities on a great number and variety of assets represents a high global risk. Essentially, this is a measure of asset vulnerability density versus enterprise prevalence of a vulnerability.

### Distinct CVEs by Vendor and Impact



Maximum of % Enterprises vs. sum of Max. Asset Count. Color shows details about Cpe (group). The marks are labeled by Cpe (group).

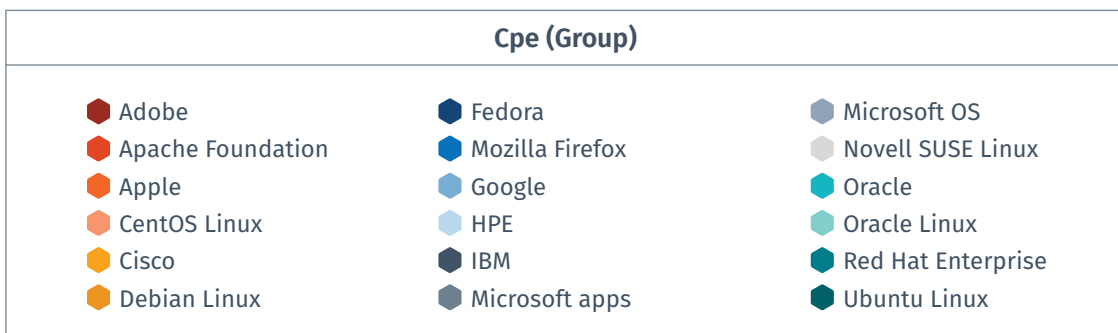


Figure 12. Distinct CVEs by vendor and impact

















# The Top 20 VULNERABILITIES

Below we list the top 20 vulnerabilities found in enterprise environments.

Where possible, we provide a CVE to help identify the vulnerability. Note: Due to the way that vulnerabilities and CVEs are aggregated in vendor patches and updates, a single vulnerability signature can detect multiple vulnerabilities, with a variety of different severities. As the update applies multiple patches, affected assets will be vulnerable to all of them if the update has not been applied. This means that some CVEs, although different and with varying severities, share the same prevalence metrics. In these cases, we have selected the vulnerability with the highest severity. If there were several that shared the same severity, we selected a representative vulnerability.





6		<p>CVE(S) NONE</p> <p>SSL Version 2 and 3 Protocol Detection. The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including an insecure padding scheme with CBC ciphers and insecure session renegotiation and resumption schemes.</p>	GROUP SSL	
7		<p>CVE(S) CVE-2018-6130</p> <p>Google Chrome out-of-bounds memory access in WebRTC.</p>	GROUP Google Chrome	
8		<p>CVE(S) CVE-2018-8242</p> <p>A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer (aka "Scripting Engine Memory Corruption Vulnerability"). This affects Internet Explorer 9-11.</p>	GROUP Microsoft IE	
9		<p>CVE(S) CVE-2017-8517</p> <p>Microsoft browsers allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers (aka "Scripting Engine Memory Corruption Vulnerability").</p>	GROUP Microsoft IE	
10		<p>CVE(S) CVE-2018-5007</p> <p>Adobe Flash Player 30.0.0.113 and earlier versions have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.</p>	GROUP Adobe Flash	
11		<p>CVE(S) CVE-2018-8249, CVE-2018-0978</p> <p>A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory (aka "Internet Explorer Memory Corruption Vulnerability").</p>	GROUP Microsoft IE	
12		<p>CVE(S) CVE-2018-8310</p> <p>A tampering vulnerability exists when Microsoft Outlook does not properly handle specific attachment types when rendering HTML emails (aka "Microsoft Office Tampering Vulnerability"). This affects Microsoft Word, Microsoft Office.</p>	GROUP Microsoft apps	
13		<p>CVE(S) CVE-2018-5002</p> <p>Adobe Flash Player 29.0.0.171 and earlier versions have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.</p>	GROUP Adobe Flash	

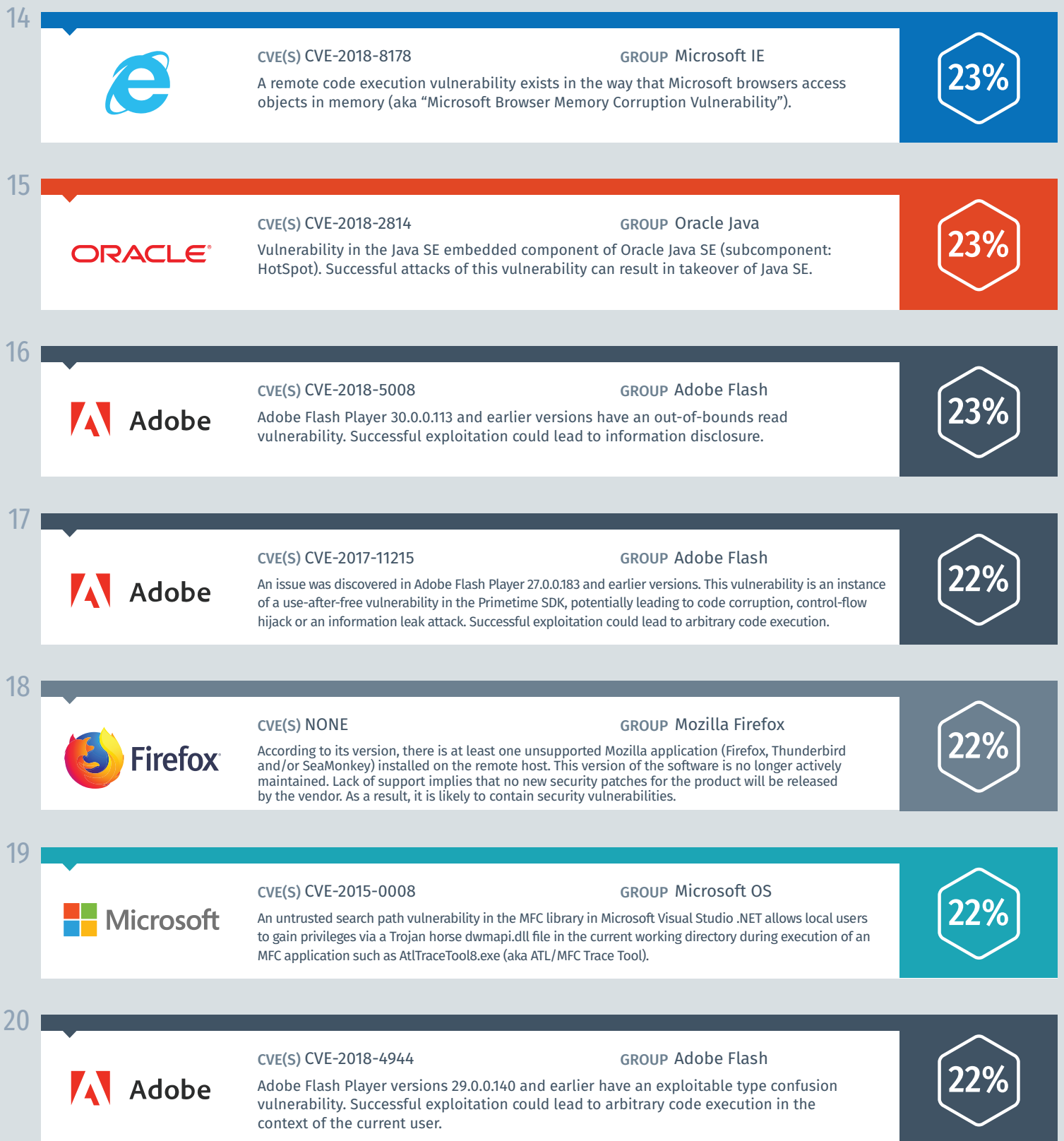


Figure 13. Top 20 Vulnerabilities Chart (percentage is based on impacted enterprises)

## CONCLUSIONS

With 61 percent of all vulnerabilities that enterprises detect in their environments rated as High severity, security organizations are challenged to determine which vulnerabilities truly represent a risk and prioritize the most critical vulnerabilities to maximize limited remediation resources. When everything is urgent, triage fails.

On average, an enterprise finds 870 CVEs across 960 assets every single day.<sup>18</sup> This means that prioritization methodologies based on remediating only High severity CVEs still leave the average enterprise with more than 548 vulnerabilities per day to assess and prioritize, often on multiple systems.

It's also interesting to see the difference between local risk and global risk. Some vendors, like Linux distributions such as Red Hat, Oracle and Novell SUSE, rank high in the amount of distinct CVEs present in an enterprise, but their impact in terms of how many organizations are affected organizations is low. These represent a local risk – high to the affected organization, but not necessarily to the greater global internet population. Of course, this risk still also depends on the precise function and context of the asset.

We also saw other vendors, such as Microsoft (.NET and Office), Adobe (Flash) and Oracle (Java), which have a comparatively low amount of distinct vulnerabilities, but affect a large number of enterprises and assets. These represent a global risk, as they affect a large number of enterprises and assets worldwide.

### Insights from the Field

As we mentioned in the previous section, every interview participant had some sort of standard protocol for prioritizing vulnerabilities for remediation, usually a combination of CVSS score and contextual data about assets and configuration. They also discussed standards for patching and remediation tasks within their organizations. All had some form of a hard deadline for remediating all vulnerabilities – a maximum amount of time a vulnerability should be allowed to persist on a system without being mitigated.

“ If some issue is open over 30 days, then people will start to get calls and a lot of attention.

“ So, we do for Criticals, we do patch within 30 days. If it is a Critical vulnerability that is highly exploitable and internet facing, it's seven days. Meaning like a Struts 2 or some of the other ones that have come out that you just have to fix immediately. For a High, it's 60 days, Medium is 90 days and Low is 120 days.

This doesn't necessarily align with our data, which shows many older vulnerabilities persisting on networks – some going back longer than a decade. Some of this discrepancy might be accounted for by internal exceptions that were also mentioned by several interviewees.

“ If something does not get addressed within that time, we require the owners – system owner, product owner, not necessarily the infrastructure owner – to fill out a risk exception form, which is a very painful process as well because they have to really provide justification to many people that sign off on those on why the exception is required.

“ For me, it's knowing the unknowns. I always ask myself the question: Have we scanned? Have we considered everything?

## WEB BROWSER AND APPLICATION VULNERABILITIES

We decided to drill down into web browser and application vulnerabilities. Client-side attacks targeting these types of vulnerabilities feature heavily in today's threat environment. These applications are generally found on clients and workstations, typically used by non-IT staff and are frequently mobile, remote and distributed.

In addition, assessing for these types of vulnerabilities requires an agent or authenticated, credentialed scanning, as this requires local system access. These factors make web browser and application vulnerabilities an intriguing area of focus.

### KEY TAKEAWAYS

Firefox High vulnerabilities dominate the top 10 web browser vulnerabilities, with **53%** of the total. This is out of proportion with its current market share of just over **10%**. Deeper analysis shows that many of the Firefox vulnerabilities present in enterprise environments are several years old. Yet, Firefox is not being updated or removed.

Oracle Java displays a similar phenomenon, with many detected vulnerabilities concentrated around 2011 to 2017. Legacy Java installations are still a root cause for persistent vulnerabilities.

Older Microsoft IE and Office vulnerabilities also feature heavily.

Adobe Flash continues this trend, despite Flash active web content having drastically declined and Adobe plans to discontinue support in 2020.

Old, discontinued and end-of-life applications are still out there in enterprise environments. Legacy applications are a major source of residual risk.

# WEB BROWSER VULNERABILITIES

Many current threats exploit client-side vulnerabilities, with web browsers high on the target list. These attacks generally work by:

- Social engineering a user into browsing a malicious website or opening a malicious file or script, which then exploits the vulnerable web browser
- Compromising a legitimate website to deploy malicious content that exploits the victim’s vulnerable web browser

Between hardened perimeters and the growing adoption of cloud technologies, attacking the user is often the most effective entry point into an enterprise. In the case of home users, it’s the only way. Financial credential and identity theft, botnets, cryptomining, ransomware, espionage and cyberextortion are all criminal activities associated with these types of attacks.

## ANALYSIS

Our data set included 1,065 unique web browser CVEs across five major vendors detected from March to August 2018:

- Apple Safari
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer (IE)
- Mozilla Firefox

**675 out of the 1065 (63%)**

web browser CVEs detected had a severity of **High**

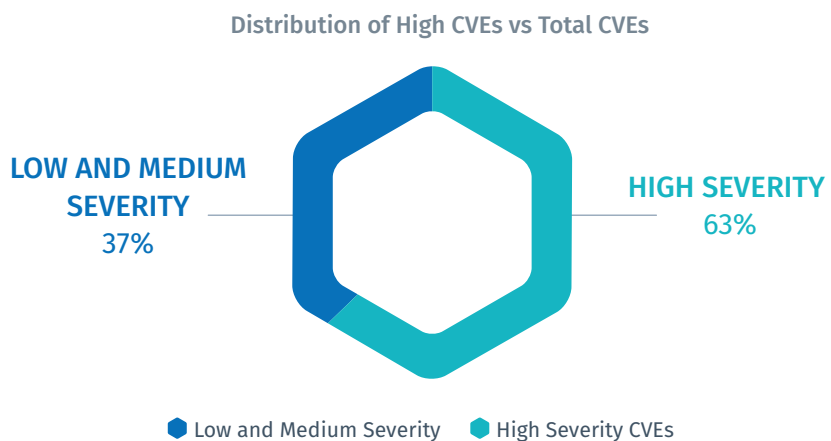


Figure 14. Distribution of High severity vs. total CVEs across all severities

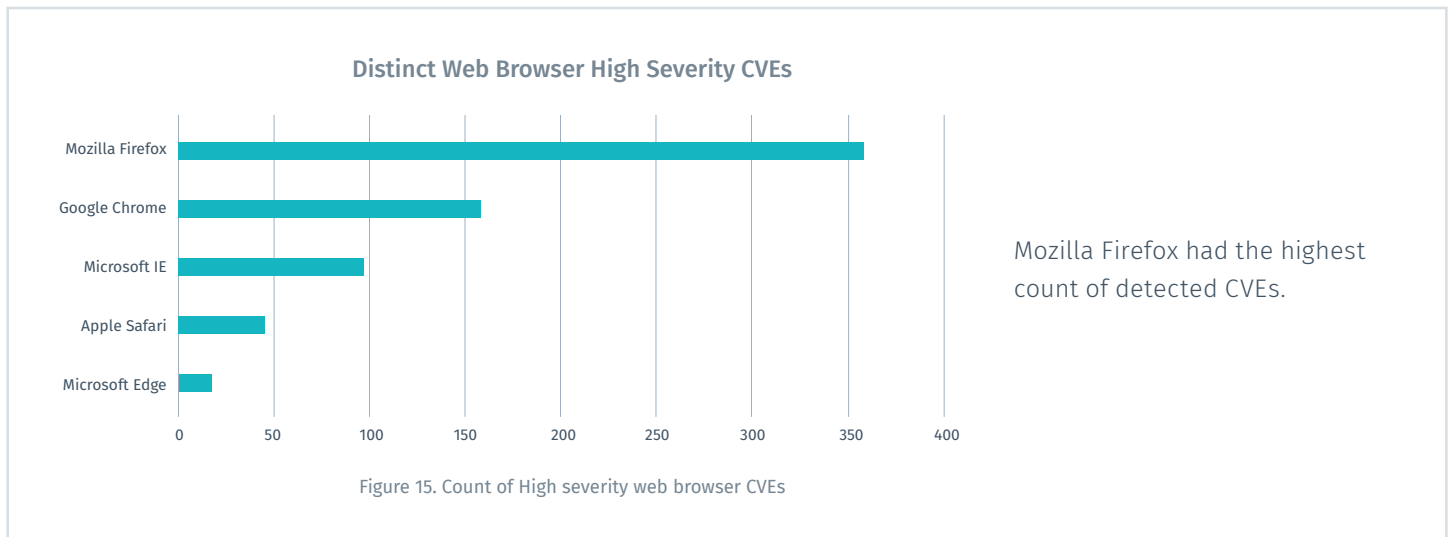
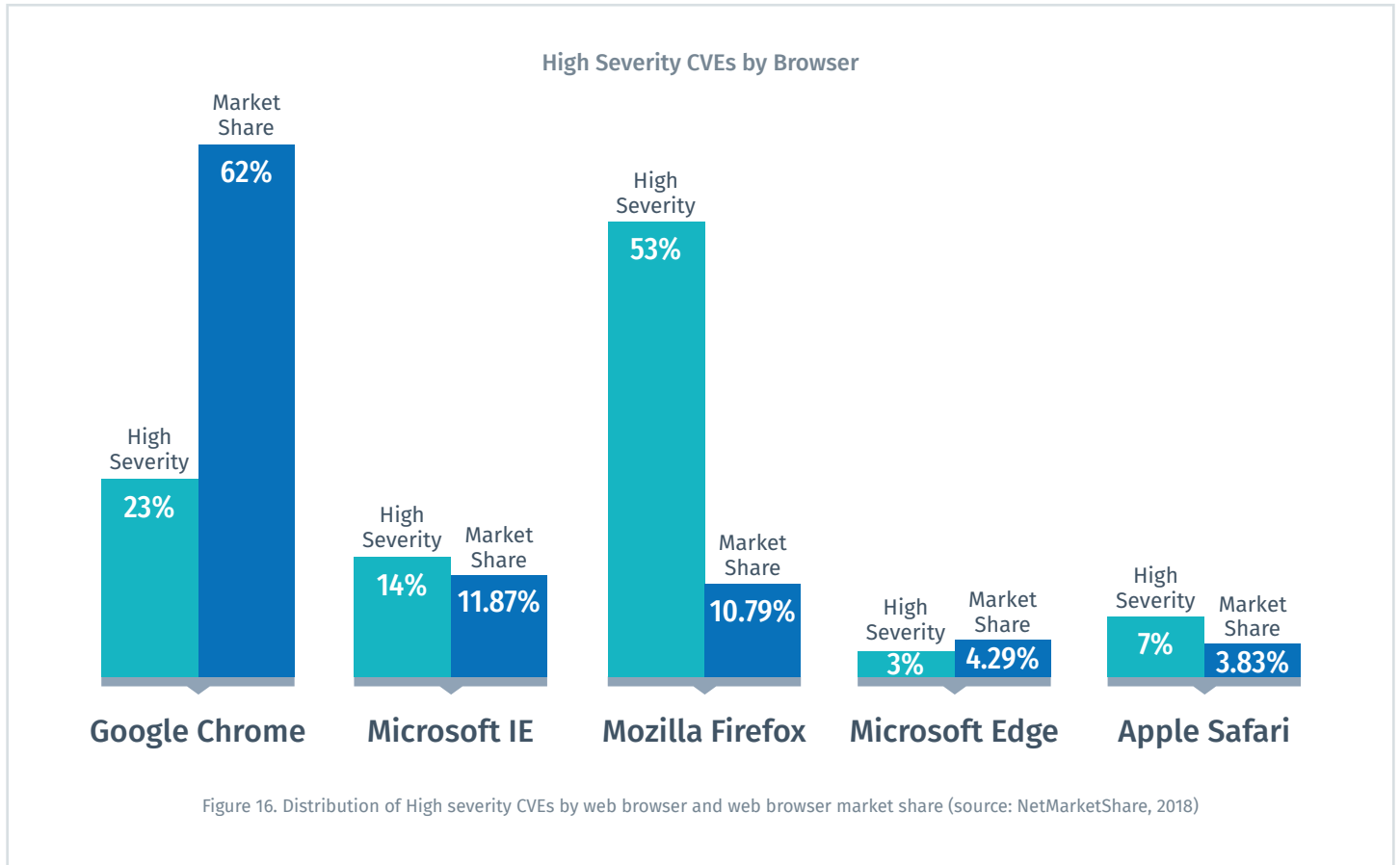


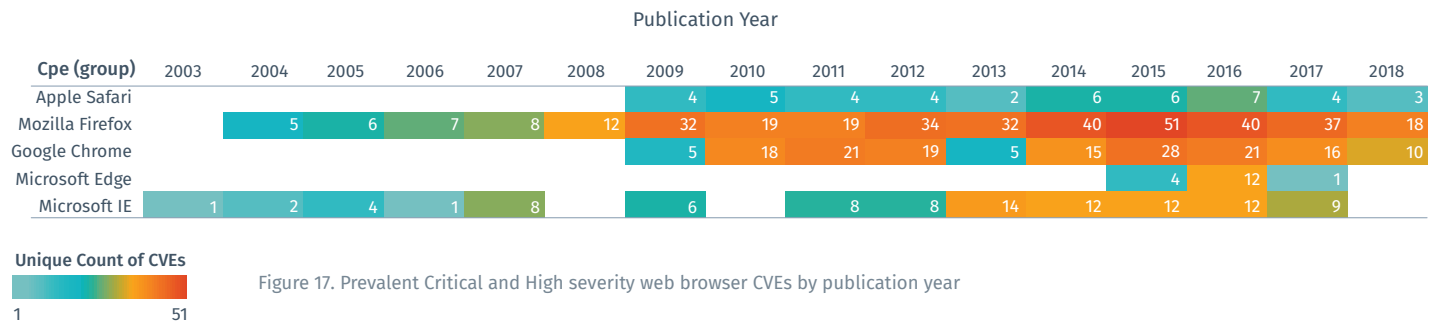
Figure 15. Count of High severity web browser CVEs

When we look at the distribution of the High severity CVEs by web browser, Firefox CVEs dominate with 53 percent of the total. Chrome comes in second, with 23 percent.



With only 10.79 percent of the browser market share, Firefox represents 53 percent of all High severity vulnerabilities. This discrepancy can partially be explained when we look at the publication years of the detected CVEs. Although Firefox has slowly been replaced by Google Chrome as the leading browser, there appear to be many older and dormant versions in the wild. Firefox vulnerabilities are not being remediated.

### Critical and High CVEs by Browser and Year



# The Top 10 WEB BROWSER VULNERABILITIES

Below we list the top 10 web browser vulnerabilities for enterprise environments.






1		<b>CVE(S) CVE-2018-6153</b> Google Chrome is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by Skia. By persuading a victim to visit a specially crafted website, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash.	<b>GROUP Google Chrome</b>	<b>30%</b>
2		<b>CVE(S) CVE-2015-6136</b> The Microsoft VBScript engines in Internet Explorer 8-11 and other products allow remote attackers to execute arbitrary code via a crafted website (aka "Scripting Engine Memory Corruption Vulnerability").	<b>GROUP Microsoft IE</b>	<b>28%</b>
3		<b>CVE(S) CVE-2018-6130</b> Google Chrome out-of-bounds memory access in WebRTC.	<b>GROUP Google Chrome</b>	<b>26%</b>
4		<b>CVE(S) CVE-2017-8517</b> Microsoft browsers allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers (aka "Scripting Engine Memory Corruption Vulnerability").	<b>GROUP Microsoft IE</b>	<b>25%</b>
5	 <b>Firefox</b>	<b>CVE(S) NONE</b> According to its version, there is at least one unsupported Mozilla application (Firefox, Thunderbird and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	<b>GROUP Mozilla Firefox</b>	<b>22%</b>



Figure 18. Top 10 web browser vulnerabilities (percentage is based on impacted enterprises)



## CONCLUSIONS

Browser market share has changed markedly over the last few years, with past leaders such as Firefox and Internet Explorer now lagging far behind Google Chrome. Sadly, vulnerabilities in these browsers have not followed the same decline, with unsupported and legacy versions in considerable numbers extant in enterprises. The age of many of these vulnerabilities is interesting because threat actors, especially exploit kit developers, are still actively targeting them.

Firefox dominates the list of most prevalent CVEs, accounting for 53 percent of all High severity vulnerabilities with only a market share of ~10 percent. The vast majority of these CVEs are between two to eight years old – with a few exceptions going back as far as 2004.

Although with a lower prevalence of 14 percent, Microsoft IE still shows up disproportionately to its market share and even in Microsoft-only businesses is being displaced by Edge. Many of the IE vulnerabilities detected between March and August 2018 were also older – in some cases going back to the last decade.

The top eight web browser CVEs affected more than 20 percent of enterprises on a single assessment day, with a high of 30 percent. That's a significant number of organizations with High severity web browser vulnerabilities in their asset population.

### Insight from the Field



**The most common reason I've seen is that these are old systems, systems that have to be around, or you just cannot retire the system because it is still holding some critical production functionality.**

# APPLICATION VULNERABILITIES

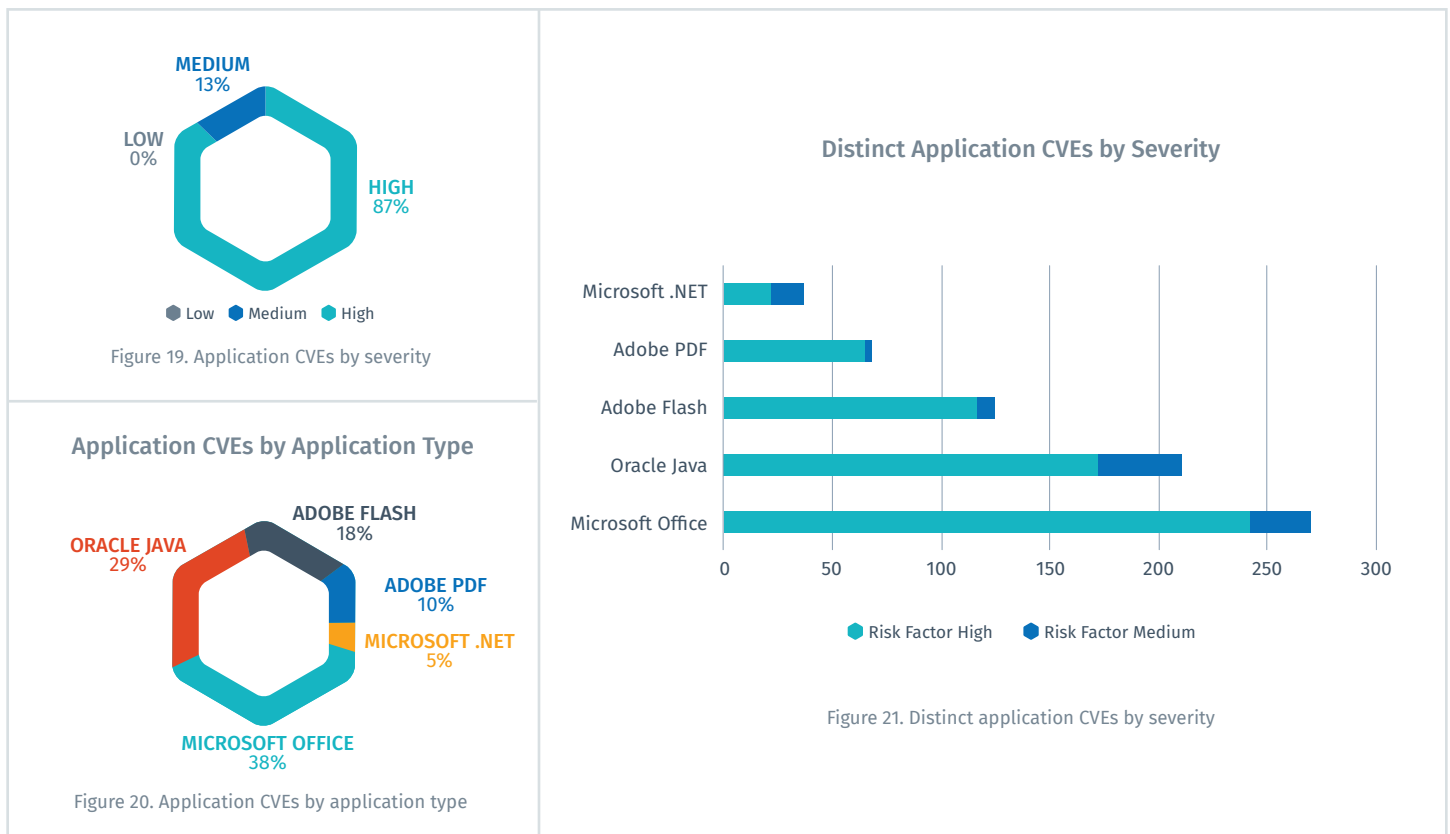
Application vulnerabilities represent another set of CVEs actively being targeted by threat actors in the wild in a variety of attacks ranging from drive-by-exploitation and cryptojacking to phishing.

These vulnerabilities are most commonly found on end-user workstations and clients. With a highly distributed and mobile workforce using a variety of platforms and operating systems, staying on top of assessing and remediating these vulnerabilities is fraught with many technical challenges.

Due to the following applications' common inclusion in exploit kits, ransomware, phishing and other attacks, we looked at:

- Adobe Flash
- Adobe PDF
- Microsoft .NET
- Microsoft Office
- Oracle Java

In total, across the five applications, 704 distinct vulnerabilities were present in enterprise environments. And, 609 of the 704 CVEs were High severity.



When we consider all CVEs detected by enterprises, Microsoft Office stands out with a large amount of distinct High severity CVEs and the biggest overall count in total. Oracle Java comes in a close second overall.

“ The other issue is that a lot of critical systems are bunched together on one system. Even though you have nine of the 10 patched, there’s one web server that cannot handle a new Java patch and everybody is stuck.

Adobe Flash and PDF are actually in the bottom half in terms of distinct CVEs detected overall in enterprise environments.

When we narrow this down to the top 20 application vulnerabilities affecting most enterprises, we see that 50 percent are Adobe Flash. Once again, we see the number of CVEs doesn't necessarily also translate to a large number of affected assets. Adobe PDF is noticeably absent from the top 20, for example. Microsoft Office does seem to buck this trend, however, coming in second in the top 20 with 20 percent – representing the highest distinct count of CVEs overall.

### Top 20 Critical and High Severity Application CVEs

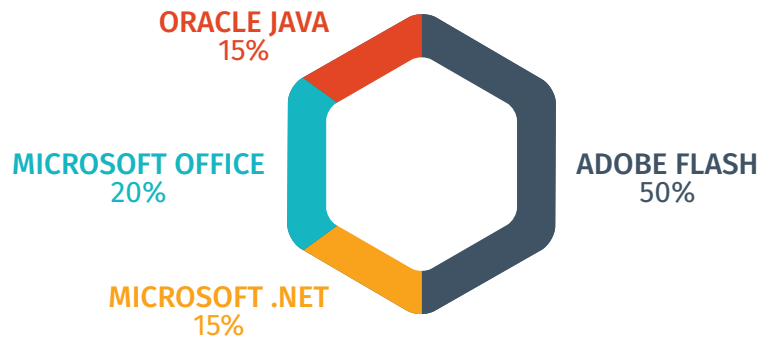


Figure 22. Distribution of applications for application vulnerabilities

When we add the vulnerability publication year in the heatmap below, we can clearly see that many Oracle Java CVEs are several years old, with concentrations in 2013, 2015 and 2017. This looks similar to the phenomenon we saw for Firefox in the web browser vulnerability breakdown – with legacy versions that have neither been updated nor removed.

### Heatmap by Distinct CVEs by Publication Date

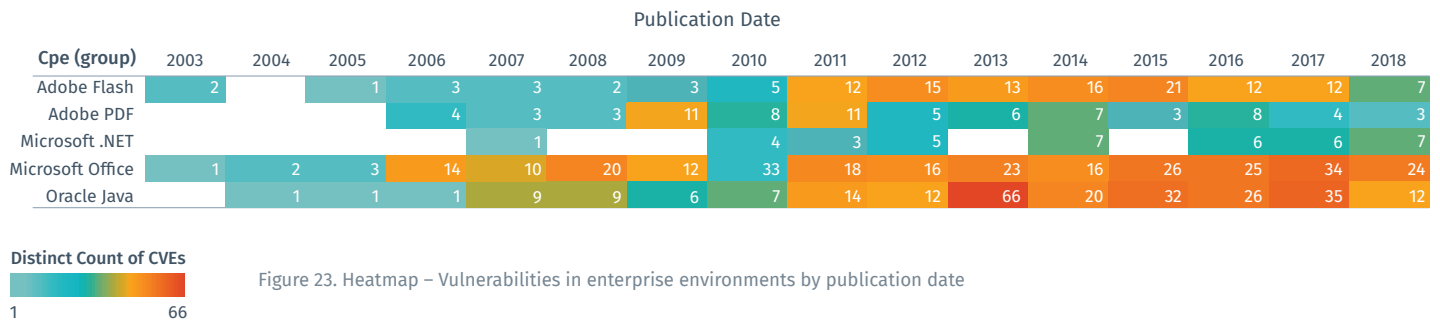


Figure 23. Heatmap – Vulnerabilities in enterprise environments by publication date

Microsoft Office applications also show a large number of older detected CVEs. There seems to be at least a superficial correlation with Microsoft Office releases,<sup>19</sup> with 2006, 2010 and 2013 prominent and a visible increase in vulnerabilities from 2016 onward.

Worryingly, there are still a considerable amount of vulnerabilities out there going back to 2006.

The breakdown below (see Figure 24) provides an overview of the total count of distinct application vulnerabilities affecting enterprise environments. For the majority of applications, the proportion of High severity vulnerabilities, versus Informational and Low and Medium severity, is more than 80 percent. For example, 82 percent of Oracle Java CVEs are rated as High.

Most common prioritization methodologies will fail at that proportion. In reality, the solution here isn't patching. Rather, it is to remove unsupported and legacy versions.

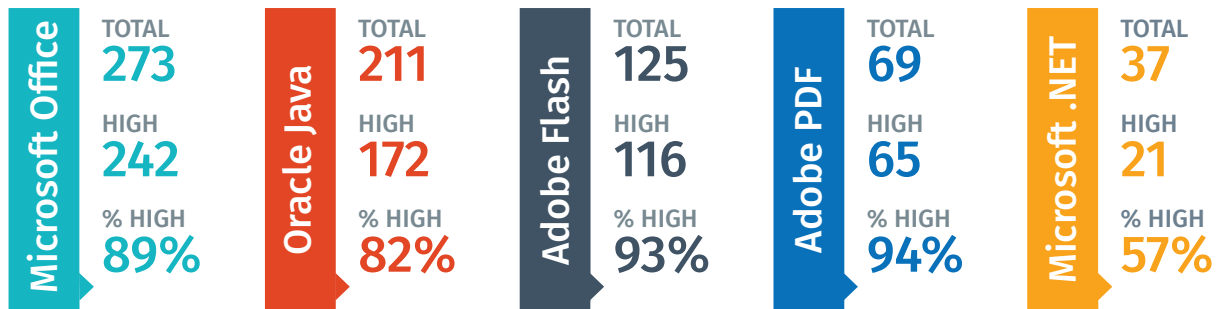


Figure 24. Distinct application CVEs in the enterprise environments

Factoring in how many enterprises and assets are actually affected by the top 10 most prevalent application vulnerabilities, we see that Microsoft .NET, Oracle Java and Adobe Flash have the most widespread impact (see Figure 25).

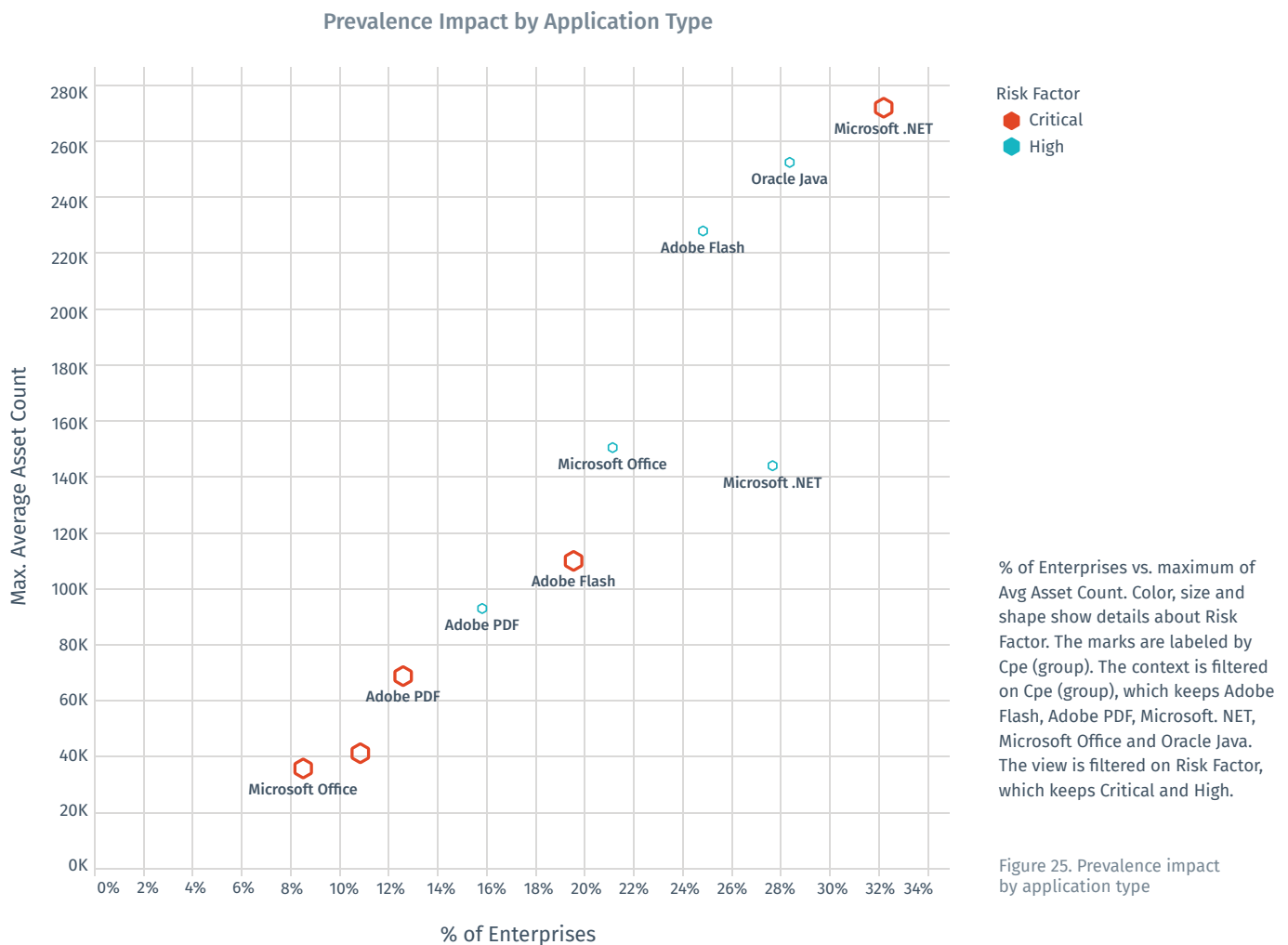


Figure 25. Prevalence impact by application type

# APPLICATION VULNERABILITIES AND EXPLOITABILITY

Correlating our prevalence data with vulnerability intelligence on exploitability (see Figure 26) paints a far more alarming picture. Public exploits are available for a whopping 79 percent of the security updates that address High severity Adobe Flash vulnerabilities and were detected as missing by enterprises in their environments. For Adobe PDF, the figure is 96 percent. For Adobe PDF, the figure is 96 percent. The lowest percentage that we have in the group is 41 percent.

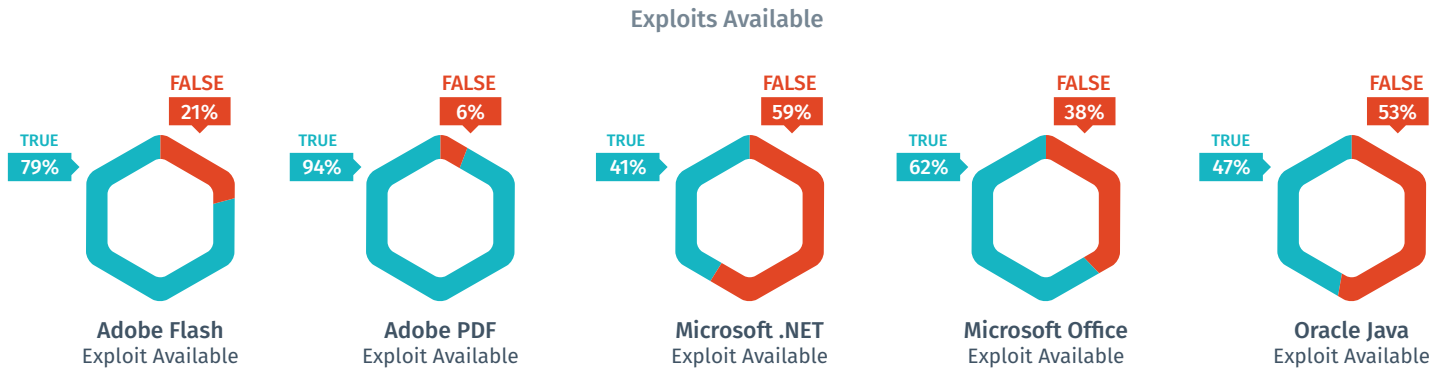


Figure 26. Application security updates and public exploit availability

As the chart below (Figure 27) shows, there are publicly available exploits for almost all Adobe Flash security updates that enterprises find missing in their environments. Considering that Flash-enabled content on the internet has steeply declined<sup>20</sup> and will be unsupported from 2020 onward, there is little value in keeping Flash installed. It does, however, represent a huge residual risk.

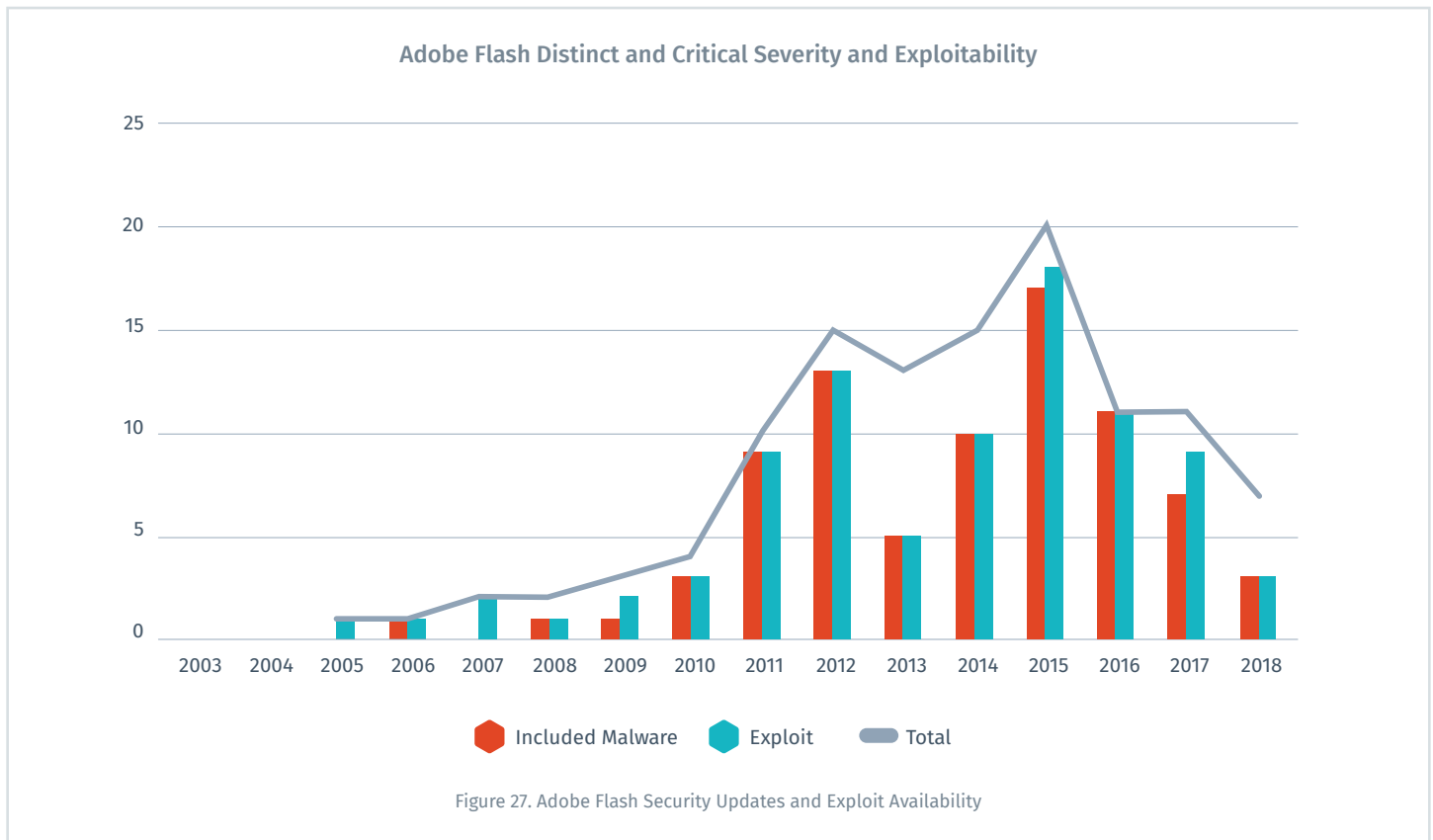







Figure 27. Adobe Flash Security Updates and Exploit Availability

# The Top 10 APPLICATION VULNERABILITIES

Below we list the top 10 application vulnerabilities for enterprise environments.

1	 <b>Microsoft</b>	<b>CVE(S) CVE-2018-8284</b> A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly (aka “.NET Framework Remote Code Injection Vulnerability”).	<b>GROUP Microsoft .NET</b>	<b>32%</b>
2	 <b>ORACLE®</b>	<b>CVE(S) CVE-2018-2938</b> Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE.	<b>GROUP Oracle Java</b>	<b>28%</b>
3	 <b>Microsoft</b>	<b>CVE(S) CVE-2018-1039</b> A security feature bypass vulnerability exists in .NET Framework that could allow an attacker to bypass Device Guard (aka “.NET Framework Device Guard Security Feature Bypass Vulnerability”).	<b>GROUP Microsoft .NET</b>	<b>28%</b>
4	 <b>Adobe</b>	<b>CVE(S) CVE-2018-5002</b> Adobe Flash Player 29.0.0.171 and earlier versions have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	<b>GROUP Adobe Flash</b>	<b>23%</b>
5	 <b>Adobe</b>	<b>CVE(S) CVE-2018-5007</b> Adobe Flash Player 30.0.0.113 and earlier versions have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	<b>GROUP Adobe Flash</b>	<b>23%</b>

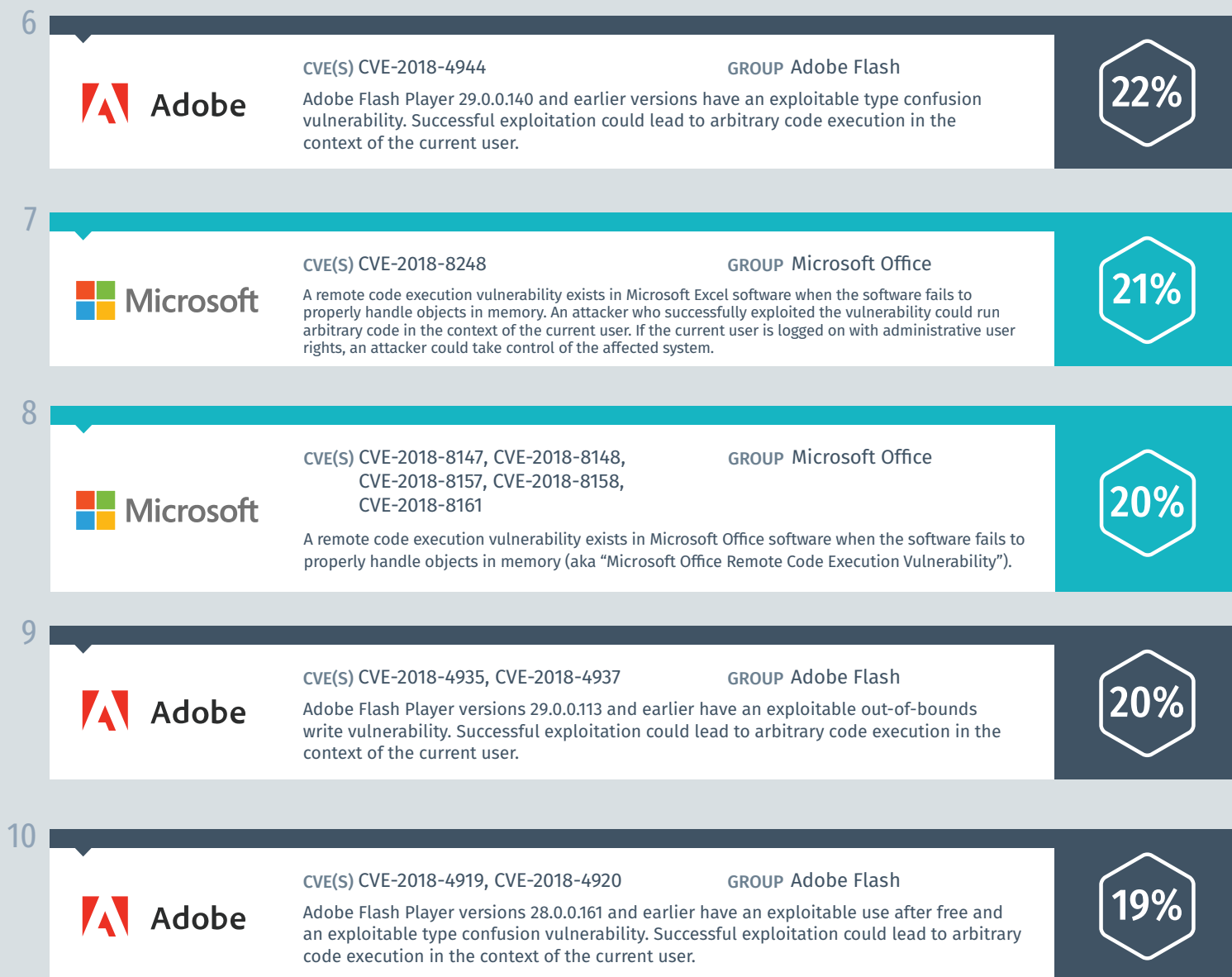


Figure 28. Top 10 Application Vulnerabilities (percentage is based on impacted enterprises)

## CONCLUSIONS

We identified many Oracle Java CVEs that are several years old, with concentrations in 2013, 2015 and 2017. This looks similar to the phenomenon we saw for Firefox in the web browser vulnerability breakdown – with legacy versions that have neither been updated nor removed.

Microsoft Office applications also show a large number of older detected CVEs. There seems to be at least a superficial correlation with Microsoft Office releases,<sup>21</sup> with 2006, 2010 and 2013 prominent and a visible increase in vulnerabilities from 2016 onward. Worryingly, there are still a considerable amount of vulnerabilities out there going back to 2006.

Public exploits are available for a whopping 79 percent of the Adobe Flash vulnerabilities detected in enterprise environments. For Adobe PDF, the figure is 96 percent. The lowest percentage that we have in the group is 41 percent. There are publicly available exploits for almost all Adobe Flash vulnerabilities that enterprises find in their environments. Considering that Flash-enabled content on the internet has steeply declined<sup>22</sup> and will be unsupported from 2020 onward, there is little value in keeping Flash installed. It does, however, represent a huge residual risk.

# High-Profile Vulnerabilities

Earlier this year, Tenable Research launched its Security Response team, providing rapid response alerting and reporting of developing and current cybersecurity events and incidents, especially those relating to vulnerabilities. Since its inception, the team has initiated a response to 40 high-profile incidents. These represent major incidents as defined by a rating scale that considers the severity, impact and prevalence of a vulnerability. We also consider whether a vulnerability exists in a key technology for a specific industry, even if it is not widely distributed.



# VULNERABILITY TIMELINE

Below is an overview of the highlights to date through August 2018. You can find the detailed reports for each of these on the [Tenable blog](#).

## '18 SECURITY RESPONSES

 **Microsoft**  
**Windows Task Scheduler Zero-Day Exploit**

Available in the wild: caution urged

Triggered by a tweet from an unhappy researcher, this privilege escalation bug was quickly exploited in the wild and leveraged by malware. Sadly, Microsoft took over two weeks to patch this issue.

AUG 28



**Apache Struts Vulnerability**

New Apache Struts vulnerability could allow for remote code execution

We blogged about yet another Struts remote RCE on August 22. Struts is very commonplace, is very difficult to patch and has been a regular source of high-profile breaches and news items. Unfortunately, there are no shortcuts to security here, knowing what you have (Zero Exposure) and disciplined patching (Best Practices) are vital!

AUG 22

**ORACLE**  
**Oracle Java/JM Database Takeover (Database)**

Oracle Database takeover using JavaVM component

AUG 15



**Foreshadow (CPU)**

New Intel speculative execution side channel vulnerabilities

AUG 14



**Faxsploit (Device)**

Remote code execution via HP fax protocols

AUG 14



**Underminer (Malware)**

Crypto coin mining via new EK vector

JULY 31



**Cisco ASA (Cisco)**

Cisco ASA/FXOS/NX-OS patched with critical patch - already being exploited

JUNE 26

On June 6, 34 patches, including five rated as critical, were released by Cisco. CVE-2018-0301 was seen exploited in the wild two weeks after the advisory was published. Cisco was our biggest source of critical security responses in early 2018.



**Apple Code Signing Flaw (Apple)**

Improper signing of third-party tools on Apple platform

JUNE 13



**Cisco ACS (Cisco)**

RCE in Cisco Secure ACS

JUNE 8



**Adobe**

**Adobe Flash Player Flaw (Adobe)**

Adobe Flash zero day being exploited in the Middle East

JUNE 7



**Zip Slip (Window Apps)**

Arbitrary file write with Zip Slip

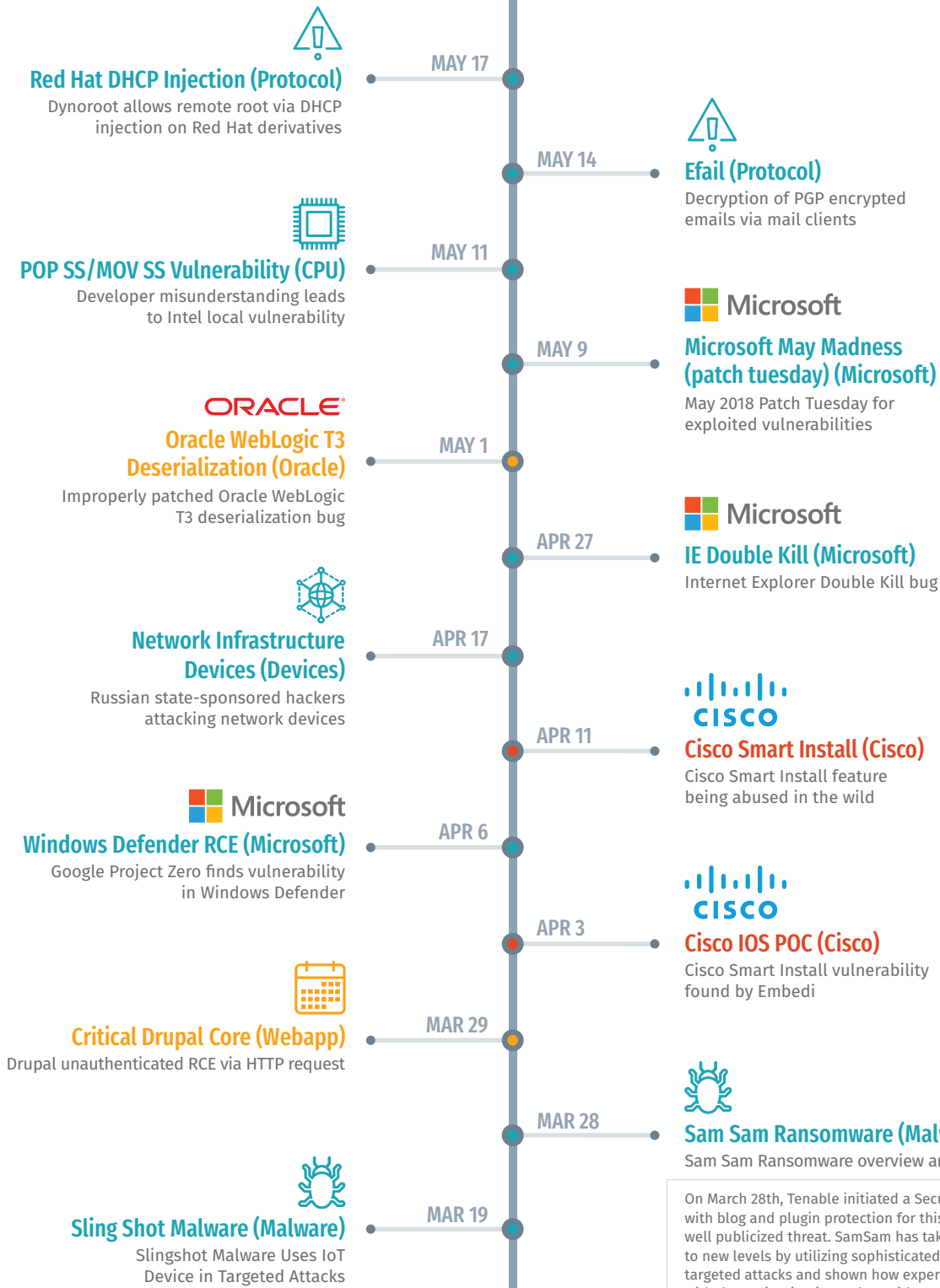
JUNE 6



**Spectre/Meltdown Variants (CPU)**

Spectre/Meltdown II

MAY 22



On March 28th, Tenable initiated a Security Response with blog and plugin protection for this unique and well publicized threat. SamSam has taken ransomware to new levels by utilizing sophisticated tools and targeted attacks and shown how experienced attackers with determination in tandem with poor security practices can be an expensive mistake.

NUMBER OF COMPANY EXPLOITS	
Cisco: 4	Protocol Issues: 4
Microsoft: 4	Oracle: 2
CPU Flaws: 3	Adobe: 1
Malware: 3	Windows Apps: 1
IoT: 2	Webapps: 1

Figure 29. Security Responses – 2018

## Insights from the Field

Vulnerabilities were big news in 2018. Starting off almost immediately, Meltdown and Spectre caused a lot of confusion and disruption in January.

“ **There was a whole bunch of panic around that at first, and then we started looking at it and the mitigations, and there was a whole lot of confusion around it. We spent a lot of time, had a lot of breakout sessions around Meltdown and Spectre, just to identify what the risks actually are. For a while, there wasn't even any proof of concept code out there [...] In terms of remote code execution, we hadn't seen any viable option for that yet. So, we kind of held fast on applying BIOS updates for a little while.**

Security practitioners reflected that this wasn't the first or last time vulnerabilities or incidents in the news forced them to adjust their vulnerability management programs. They tied these adjustments to a few different priorities. In some cases, it was about ensuring the CISO or CIO was prepared to field questions from other executives, customers and the media.

“ **They hear something on the news and they go, 'Now I'm going to get questions off these when I go in and I don't want to look like an idiot because cyber is reporting to me. So, I have to look like I'm on top of things.' And oftentimes for them, they don't care really what the security issue is, it's very much about how it impacts them directly.**

In other cases, it was about ensuring the organization wasn't going to be surprised by an attacker based on a known vulnerability.

“ **You know, when something like Struts 2 comes out, we have corporate initiatives where we reach out to all business units and you're talking about different resources, different technologies and you're asking, 'Are we susceptible to this vulnerability across the company?' You know as large as, for example, ours is, it's one of those things where it takes a lot of resources to figure that out – unless you have a program that's in place that can handle it.**

# Contributors

## PRIMARY RESEARCH

Paul Davis, High-Profile Vulnerabilities

Oliver Rochford, Research Design and Data Analysis

Lucas Tamagna-Darr, CVE and CVSS Trend Data

Claire Tills, Qualitative Research

Andrew Tracey, Data Science

## SUBJECT MATTER EXPERTS

Anthony Bettini, Sr. Director of Engineering

Rajiv Motwani, Director of Research, Vulnerability Detection

Thomas Parsons, Sr. Director of Product Management

# Appendix

## CVSS SEVERITY RATINGS

Throughout the document, we make reference to “severity” and “severity rating.” The table below translates the descriptive severities into numerical CVSS scores. CVSSv2 officially does not recognize a severity rating of Critical.

CVSS v2.0 Ratings	
Severity	Base Score Range
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	7.0 - 10.0

CVSS v3.0 Ratings	
Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

## CVE DISCLOSURE YEARS

While 15,038 CVEs have been published under the CVE-2017-XXXX identifier, some of these have been published in 2018. 10,959 CVEs were actually published in 2017. This provides some insight into the current CVE backlog.

# Methodology

## DATA SET

The data set is composed of vulnerability prevalence data:

- For a period from March to August 2018
- Containing more than 900,000 vulnerability assessments
- From 2,100 individual enterprises
- From 66 countries

We used this data set to determine the most prevalent vulnerabilities.

## PREVALENCE

We calculated “prevalence” based on highest maximum count of affected enterprises on a specific scan day. We selected affected enterprises, rather than affected asset count, because we wanted a measure that allowed us to determine how many organizations had to deal with a vulnerability. Basing prevalence on the count of affected assets would mean that some technologies (e.g., network devices or servers) would inevitably not make the top listing. Most enterprises have thousands of Windows workstations, but only dozens or hundreds of servers. But, almost every enterprise has servers and workstations, in general.

We used the highest one-day count of affected enterprises to obtain a clear indication of scale and eliminate the need to account for anomalies in working with averages and vulnerabilities of different ages.

For the proportion of affected enterprises, we have a total enterprise count (N) of 2,100.

## CVES VERSUS VULNERABILITIES

Vulnerabilities are not strictly speaking CVEs. A single vulnerability may receive multiple CVEs. For example, unique CVEs for the same vulnerability exist for a variety of OSs (e.g., Firefox on Windows, Red Hat Linux or SUSE Linux). We decided to count every CVE as a distinct vulnerability. From an enterprise point of view, they are different vulnerabilities because they require different patches or remediation steps.

We use anonymized telemetry data collected from our Tenable.io® platform in accordance with our end-user license agreement (EULA) to research trends and topics fundamental to cybersecurity. We do not use telemetry data from other Tenable products, like Nessus® or SecurityCenter®, in our research and related reports.

## INTERVIEW METHODOLOGY

To add a real-world perspective to this data, we also conducted 12 interviews with security practitioners at both the manager and analyst level. These hour-long conversations focused on vulnerability management strategy and practice to better understand how certain “best practices” play out in reality. Questions were focused on key performance indicators for vulnerability management like scanning frequency and time to remediate as well as higher-level strategic questions about how security teams work within complex organizations. The interviews were analyzed using both descriptive and pattern coding. Initial categories were based on themes for the report.

# Endnotes

1. CVE is maintained by the [MITRE Corporation](#)
2. <https://cve.mitre.org/>
3. See [Appendix](#)
4. Based on Tenable Intelligence
5. Primary Research, Tenable Vulnerability Intelligence
6. <https://www.tenable.com/blog/the-equifax-breach-a-cyber-wtf-moment>
7. <https://www.tenable.com/blog/wannacry-three-actions-you-can-take-right-now-to-prevent-ransomware>
8. "State of Security Response," Ponemon/ServiceNow, 2018
9. <https://www.tenable.com/blog/quantifying-the-attacker-s-first-mover-advantage>
10. <https://www.tenable.com/blog/how-mature-are-your-cyber-defender-strategies>
11. "State of Security Response," Ponemon/ServiceNow, 2018
12. <https://www.csoonline.com/article/3300753/security/congress-pushes-mitre-to-fix-cve-program-suggests-regular-reviews-and-stable-funding.html>
13. <https://nvd.nist.gov/>
14. Example of an academic study on this topic: <https://www.sciencedirect.com/science/article/pii/S2210832717302995>
15. <https://nvd.nist.gov/vuln/detail/CVE-2017-1000391>
16. <https://jenkins.io/security/advisory/2017-11-08>
17. Based on Tenable Intelligence
18. Based on Tenable Intelligence
19. [https://en.wikipedia.org/wiki/History\\_of\\_Microsoft\\_Office](https://en.wikipedia.org/wiki/History_of_Microsoft_Office)
20. <https://www.bleepingcomputer.com/news/security/google-chrome-flash-usage-declines-from-80-percent-in-14-to-under-8-percent-today/>
21. [https://en.wikipedia.org/wiki/History\\_of\\_Microsoft\\_Office](https://en.wikipedia.org/wiki/History_of_Microsoft_Office)
22. [https://www.theregister.co.uk/2017/07/25/flash\\_naruh\\_internets\\_screen\\_door\\_gone\\_for\\_good\\_by\\_2020](https://www.theregister.co.uk/2017/07/25/flash_naruh_internets_screen_door_gone_for_good_by_2020)

 **tenable** | RESEARCH

7021 Columbia Gateway Drive  
Suite 500  
Columbia, MD 21046

North America +1 (410) 872-0555

[www.tenable.com](http://www.tenable.com)

11/18 V01

Copyright 2018 Tenable, Inc. All rights reserved. Tenable, the Tenable logo, Tenable.io, and The Cyber Exposure Company are registered trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.