

TENABLE'S 2020 THREAT LANDSCAPE RETROSPECTIVE

A guide for security professionals to navigate
the year in vulnerabilities

Table of Contents

FOREWORD	3
EXECUTIVE SUMMARY	4
INTRODUCTION	7
SECTION 1: OVERVIEW OF THE 2020 VULNERABILITY LANDSCAPE	8
Noteworthy Vulnerabilities: What’s in a Name?	10
Zero-Day Vulnerabilities	11
Vulnerability Season	12
COVID-19 and the Remote Workforce.....	13
SECTION 2: OVERVIEW OF THE 2020 THREAT LANDSCAPE	17
Ransomware remains a prominent root cause of healthcare breaches.....	18
U.S. government issues alerts on VPN vulnerabilities and foreign threat actors...	19
SECTION 3: A CLOSER LOOK AT THE KEY VULNERABILITIES IN 2020	21
Apache, Apple, Cisco, Citrix, F5 Networks, Fortinet, Google, Microsoft, Mozilla, Open Connectivity Foundation, Operating Systems (Windows and Linux), Oracle, Palo Alto Networks, Pulse Connect, SAP, Sophos, TCP/IP Libraries, Trend Micro, vBulletin, VMWare	
CONCLUSION	41

Foreword

Looking Forward By Looking Back

If there is any bright spot to be found in the tumultuous global events of 2020, perhaps it is the realization of our shared human connectedness. As many organizations embraced a work-from-home model in response to the COVID-19 pandemic, our business lives and our family lives converged in sometimes messy ways – and helped us all see one another with that much more compassion.

The events of 2020 also made clear how reliant we all are on the infrastructure and supply chains underpinning modern society – agriculture, food and beverage manufacturing, pharmaceutical development – particularly in times of crisis. The software supply chain itself came under renewed scrutiny as a result of the SolarWinds breach, which was disclosed in mid-December.

While full ramifications of the SolarWinds breach were still under investigation as of January 5, 2021, when this report was finalized, this incident makes one thing crystal clear: defense in depth is the foundation to defend oneself against intrusion. Each device, each asset in the infrastructure needs to be considered as potentially becoming rogue, and we need to continue to minimize the privileges they have and the attack surface to which they have access. While few organizations would have the wherewithal to prevent a breach as sophisticated as SolarWinds, sound cyber hygiene practice can help to thwart any lateral movement that might occur as a result of the breach. We'll continue to monitor the developments in the case on [the Tenable blog](#).

If 2020 ended at a crossroads for infosec management, then 2021 will be the time for choosing the path that leads to a risk-based approach to vulnerability management. As the attack surface expands, vulnerability management has a central role to play in modern cybersecurity strategies. Unpatched vulnerabilities leave sensitive data and critical business systems exposed, and represent lucrative opportunities for ransomware actors. Modern vulnerability management requires identifying unnecessary services and software, limiting third-party code, implementing a secure software development lifecycle and practicing accurate asset detection across your entire attack surface, including information technology, operational technology and internet of things, regardless of whether they reside in the cloud or on premises.

Tenable Research seeks to step out in front of the curve of the vulnerability management cycle. Our Security Response Team (SRT) tracks threat and vulnerability intelligence feeds to make sure our plugin teams can quickly deliver coverage to our products. The SRT also works to dig into technical details and test proof-of-concept attacks to ensure customers are fully informed of the risks.

Reducing the cyber exposure gap requires a broad understanding of the threat landscape. Tenable Research takes that approach to equip our customers and the industry at large with the tools, awareness and intelligence to effectively reduce risk. To further those goals, the SRT has compiled this 2020 Threat Landscape Retrospective, which offers both a macro look at the trends that shaped the year as well as a detailed compendium of key vulnerabilities. The insights and data provided in these pages are designed to help cyber defenders learn from the past in order to build cybersecurity strategies that protect critical infrastructures, supply chains and data while respecting privacy.

Renaud Deraison

Co-founder and Chief Technology Officer

Tenable

Executive Summary

Each day, cybersecurity professionals around the world face a fresh stream of vulnerabilities that could place their organizations at risk. The scale and scope of the challenge is staggering – particularly in light of the ever-expanding attack surface of IT, operational technology (OT) and internet of things (IoT) devices – and the rush to prioritize and remediate the next new threat leaves little time for reflection. Remediation needs to be handled with a risk-based approach, with a clear understanding of the impact patching will have on business operations, before deploying to a live environment. This is no small task for an organization of any size and can be especially difficult for those with large and diverse environments.

Pausing for a retrospective may feel like a luxury few can spare the time for. Yet, as we prepare to face the new cybersecurity challenges looming in 2021, we believe taking the time for a look back can provide valuable lessons and important context to help cybersecurity professionals identify gaps in their practices and refine their strategies with an eye toward improving their risk-based approach to vulnerability management.

It is with these goals in mind that Tenable's Security Response Team assembled the 2020 Threat Landscape Retrospective (TLR). The TLR offers an overview of the key vulnerabilities disclosed or exploited in the 12 months ending December 31, 2020. In this report, we explore:

- The implications of the COVID-19 pandemic from a cyber defender perspective;
- The notable increase in severe vulnerabilities reported during the summer months;
- The implications behind a series of alerts from the U.S. government warning about the dangers of unpatched vulnerabilities;
- Trends observed in ransomware and breaches; and
- Details of the key vulnerabilities affecting enterprise software.

Key Stats

18,358

New CVEs
Assigned in 2020

730

Public Breach
Events Identified*

22B

Records Exposed*

35%+

of Zero-Day
Vulnerabilities Are
Browser-Based

18

Ransomware
Groups Operate
Leak Websites

TOP 5 VULNERABILITIES IN 2020

1

ZEROLOGON

CVE-2020-1472

2

CITRIX ADC/
GATEWAY/SDWAN
WAN-OP

CVE-2019-19781

3

PULSE CONNECT
SECURE SSL VPN

CVE-2019-11510

4

FORTINET
FORTIGATE SSL VPN

CVE-2018-13379

5

F5 BIG-IP

CVE-2020-5902

* Up to October 30, 2020

9 Key Takeaways



Yearly CVE Count Continues to Jump Around

From 2015 to 2020, the number of reported CVEs increased at an average annual percentage growth rate of 36.6%. The 18,358 CVEs reported in 2020 represent a 6% increase over the 17,305 reported in 2019 and a 183% increase over the 6,487 disclosed in 2015. The fact that for the last three years we have seen over 16,000 CVEs reported annually reflects a new normal for vulnerability disclosure. For the average security professional, prioritizing which of these vulnerabilities warrants your attention is more challenging than ever, and not all vulnerabilities are created equal.



You Can't Judge a Book by the Cover

"Headline" vulnerabilities tend to be the ones that attract the most attention from the media and business leaders, putting pressure on security professionals to respond even if the threat to the business is low. Our review of high-profile vulnerabilities in 2020 reveals that not every critical vulnerability had a name and logo given to it. Conversely, not every vulnerability with a name and logo should be seen as critical. Other factors must be considered when weighing the severity of a vulnerability, including the presence of proof-of-concept (PoC) exploit code and ease of exploitation.



Cybercriminals Love Sittin' on Chrome

Web browsers like Google Chrome, Mozilla Firefox, Internet Explorer and Microsoft Edge are the primary target for zero-day vulnerabilities, accounting for over 35% of all zero-day vulnerabilities exploited in the wild. Considering that the browser is the gateway to the internet, patching these assets is essential to the security of your enterprise network.



Forgot About VPNs

Pre-existing vulnerabilities in virtual private network (VPN) solutions — many of which were initially disclosed in 2019 or earlier — continue to remain a favorite target for cybercriminals and nation-state groups. Organizations that have yet to prioritize patching these flaws are at extreme risk of being breached. Add in the dramatic workforce changes necessitated by the COVID-19 pandemic and it's clear that securing your VPN solutions is more critical than ever.



Remote Workforce Raises New Levels of Concern

In response to COVID-19, the unprecedented shift for businesses and schools to remote work and distance learning has created a brand new set of security challenges. From relying on tools such as VPNs and remote desktop protocol (RDP) to introducing new applications for video conferencing, these new solutions raise concerns that can only be addressed through diligent patching and implementing the right security controls.



Everything Old Is New Again

It's a lesson you've heard before: patch your critical vulnerabilities. Throughout 2020, it was the U.S. government sounding this familiar alarm, issuing several warnings about the risk posed by unpatched vulnerabilities. Nation-state groups continue to actively leverage these flaws to target the public sector. These alerts should serve as a reminder of just how important it is to patch vulnerabilities in a timely manner.



Can't Unwind in the Summertime

Summer 2020 saw 547 vulnerabilities disclosed, including a number of critical vulnerabilities over the course of a three-month period, creating challenges for IT administrators and staff tasked with triaging patching priorities as they sought to protect their organizations from a barrage of new threats. The sudden influx of vulnerabilities, dubbed by some as "CVE Season," revealed the need for security teams to implement a risk-based approach to remediation.



For Ransomware, Extortion Is the Key

Ransomware remains the most disruptive global cyberthreat. This year, a new array of extortion tactics, such as operating leak websites to name and shame victims, are proving to be lucrative for attacker groups looking to secure ransom demands. This threat affects virtually every industry and stems from a variety of root causes all of which security teams must account for in their defender strategy.



Protect Ya Neck to Prevent Breaches

Data breaches are on the rise and the consequences to your organization can be severe. Analysis of breach data from January through October 2020 shows 730 publicly disclosed events resulting in over 22 billion records exposed, not to mention the untold damage to reputation and trust. Furthermore, over 35% of breaches are linked to ransomware attacks, resulting in an often tremendous financial cost. Breaches affect hundreds of organizations every year and the number of exposed records grows with each new affected party.

Methodology

This report was compiled based on events we've analyzed as well as blogs we've published over the course of 2020. We utilized information from advisories published by U.S. government agencies throughout the year. Our breach data was compiled by collecting publicly available information from national and local news outlets reporting on data breaches from January through October 2020.

How to use this report

- Identify and patch any of the vulnerabilities referenced in this report
- Understand some of the pitfalls from the shift to the remote workforce
- Learn how ransomware gangs are breaching organizations and the tactics they're employing to extract ransom demands
- Learn some of the common ways data breaches occur and what your organization can do to prevent them from happening

Introduction

Throughout the year, Tenable's Security Response Team tracks and reports on vulnerabilities and security incidents, providing guidance to security professionals as they plan their response strategies. Our work gives us the opportunity to closely observe the ever-changing dynamics of the threat landscape. As organizations around the world prepare to face the new cybersecurity challenges looming in 2021, we believe it's crucial to pause and take a look back at the most critical vulnerabilities and risks from the past year. Understanding which enterprise systems are affected by the year's vulnerabilities can help organizations understand which flaws represent the greatest risk.

In [Section 1](#), we explore the trends that shaped the vulnerability landscape in 2020, including:

- Which headline vulnerabilities represented the greatest risk;
- The influence of zero-day vulnerabilities on the threat landscape; and
- The many ways attackers exploited the global response to the COVID-19 pandemic.

In [Section 2](#), we explore the trends that shaped the threat landscape in 2020, including:

- A closer look at the root causes of the year's breaches;
- The latest ransomware trends; and
- A recap of SolarWinds and other significant threats featured in government alerts.

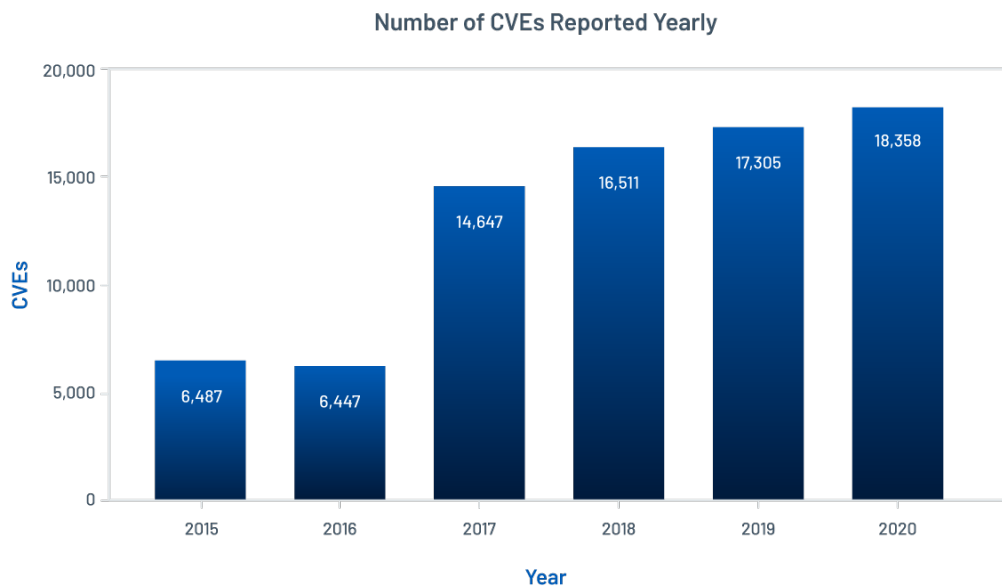
In [Section 3](#), we provide a detailed list of key vulnerabilities affecting a wide range of vendors, including:



SECTION 1

An Overview of the 2020 Vulnerability Landscape

Each year, security researchers and internal research teams disclose tens of thousands of vulnerabilities in a variety of software products used for business. From 2015 to 2020, the number of reported CVEs increased at an average annual percentage growth rate of 36.6%. The 18,358 CVEs reported in 2020 represent a 6% increase over the 17,305 reported in 2019 and a 183% increase over the 6,487 disclosed in 2015.



Source: [National Vulnerability Database \(NVD\)](#) as of January 5, 2021

Even with the plethora of vulnerabilities disclosed in 2020, it's important not to overlook so-called "legacy vulnerabilities" from prior years, which continue to be a valuable asset to cybercriminals while posing a challenge for defenders. Some of the most prominent vulnerabilities exploited in 2020 were VPN flaws for which patches had been issued in 2019. These vulnerabilities, though old, continue to be **actively exploited by threat actors** and were on the list of **top vulnerabilities targeted by state-sponsored actors** according to the U.S. government. We believe these three "legacy" VPN vulnerabilities are particularly worth addressing (more details on each can be found in Section 3):

1. CVE-2018-13379: Fortinet FortiOS SSL VPN Web Portal Information Disclosure
2. CVE-2019-11510: Arbitrary File Disclosure in Pulse Connect Secure
3. CVE-2019-19781: Citrix Application Delivery Controller (ADC) and Gateway

One of the common threads across these three vulnerabilities is the fact that they are all directory traversal flaws. As its name implies, a directory traversal vulnerability allows an attacker to traverse the directory tree to access files outside of the parent folder. An attacker can accomplish this by sending a specially crafted request containing a directory traversal string (e.g. "../../../") to vulnerable endpoints. This would enable an attacker to potentially read sensitive information or write to the underlying disk in a limited fashion. This type of vulnerability has been around for over two decades and it appears that a variety of software applications are susceptible to directory traversal flaws in 2020. We fully expect more directory traversal vulnerabilities to be discovered in the years ahead.

Of course, 2020 offered no respite from new VPN vulnerabilities, including [CVE-2020-5135](#), a critical pre-authentication stack-based buffer overflow vulnerability in the [SonicWall VPN Portal](#) as well as a series of [actively exploited Citrix vulnerabilities](#) that could be used to extract VPN session details, both of which are detailed later in this report. The recurring theme of discovering VPN vulnerabilities and subsequent exploitation highlights the urgency to prioritize patching VPN systems.

The COVID-19 pandemic and the resulting move to a remote workforce for many organizations around the world put even greater emphasis on the importance of VPNs in 2020. IT administrators working over VPN may have to prioritize what work is carried out, including patching cycles due to limited VPN bandwidth as some patches can be quite substantial. VPNs, while providing a secure connection for working remotely, can themselves be vulnerable if not patched accordingly. Even with the prospect of a COVID-19 vaccine in the near future, many companies are continuing to reevaluate the future of remote work. Some organizations are planning to shift to a fully remote workforce, welcoming a new working normal, while others are hopeful for a return to the office in 2021. In some cases, organizations may look to adopt a hybrid model. Whichever form of remote work a business decides to adopt, maintaining a secure remote connection and protecting core assets becomes vital. We further explore the impact of COVID-19 on the threat landscape later in this section.

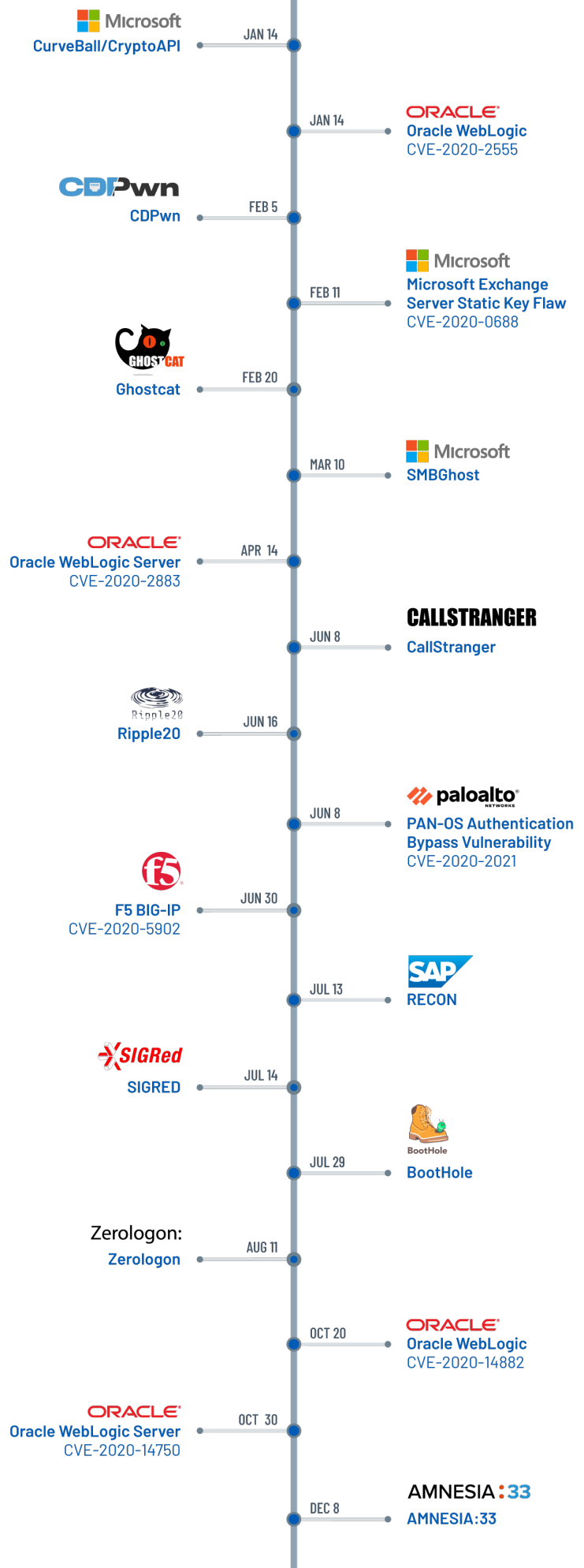
Each year, an increasing number of high-profile data breaches are disclosed across a variety of industries and 2020 was no exception. Most notably, in December an unprecedented breach was announced, caused by a backdoor placed by nation-state threat actors in the SolarWinds Orion Platform. We explore the impact of this and other breaches further in Section 2.

THE COVID-19 PANDEMIC AND THE RESULTING MOVE TO A REMOTE WORKFORCE PUT EVEN GREATER EMPHASIS ON THE IMPORTANCE OF VPNs IN 2020

Noteworthy Vulnerabilities: What's in a Name?

In this veritable sea of vulnerabilities, one way that vulnerabilities rise above the tide to gain attention is to receive their own specialty name. These names are sometimes given to a vulnerability, or a class of vulnerabilities, by the researchers who discovered them. At other times, names are bestowed by the broader security community. Named vulnerabilities may also get their own logo to go along with the name.

The severity of these named vulnerabilities is relative: Just because a vulnerability has a name and/or logo doesn't mean it is worthy of your attention more than other, unnamed vulnerabilities. However, there are some that definitely warrant it. Likewise, some vulnerabilities remain nameless and logoless yet are critical to remediate quickly. To help navigate these waters, the timeline on this page reveals the vulnerabilities we've determined to be the most noteworthy ones disclosed in 2020 based on the availability of PoC code, exploitation status and potential impact. More details on each of these can be found in Section 3.

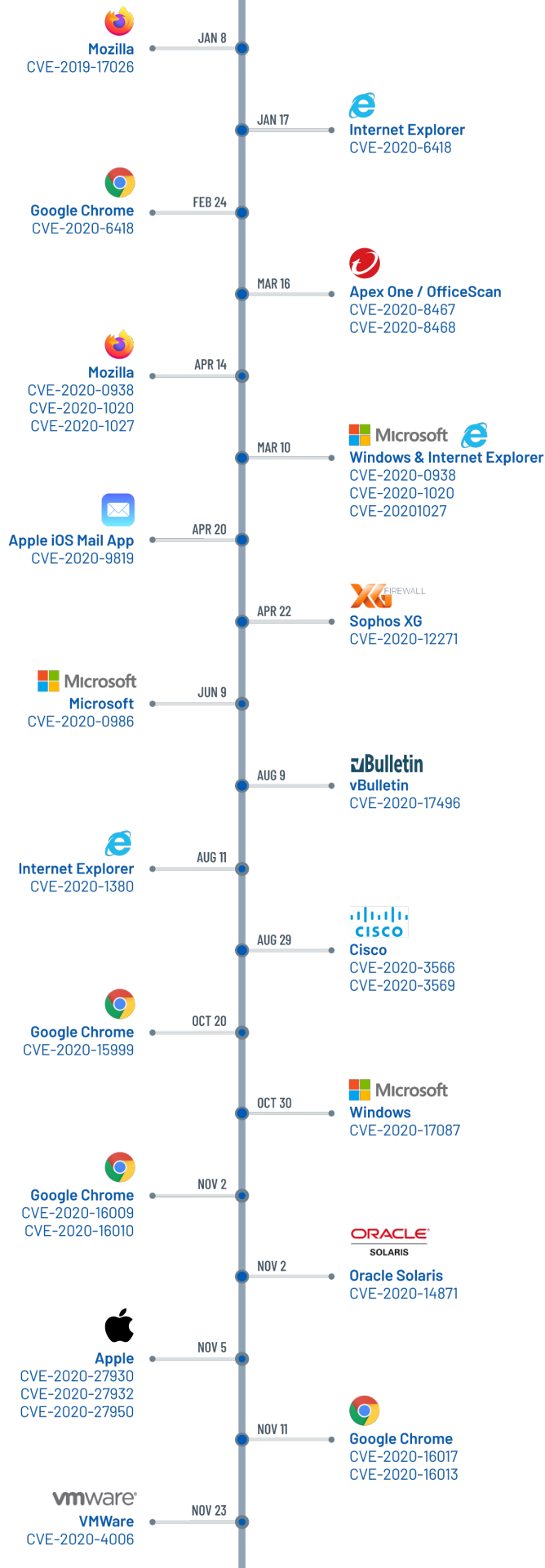
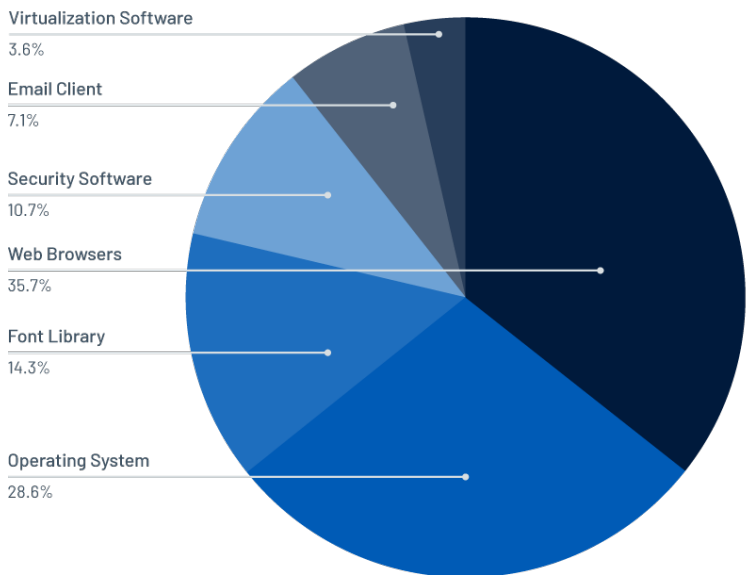


Zero-Day Vulnerabilities

Outside of noteworthy vulnerabilities, the one constant each year is the discovery of zero-day vulnerabilities. Zero-day vulnerabilities are typically announced in an out-of-band advisory or research post and pose a challenge for security professionals. In deciding a strategy for mitigating a zero-day, an organization must weigh the impact the vulnerability could have on their environment, how prevalent it is in their organization and the likelihood of exploitation by threat actors.

There were a total of 29 zero-day vulnerabilities disclosed in 2020. We identified these vulnerabilities based on disclosures made by security researchers and in-the-wild exploitation identified by vendors throughout the year. Of the 29 vulnerabilities, over 35% were browser-related vulnerabilities. While browser-based vulnerabilities are easy enough to consider prioritizing in the remediation process due to their ease of patching, they do not necessarily carry the greatest risk. Devices such as firewalls, domain controllers and VPNs could have a significantly greater impact if compromised and more care is needed when testing and applying patches or mitigations. More details on these vulnerabilities can be found in Section 3.

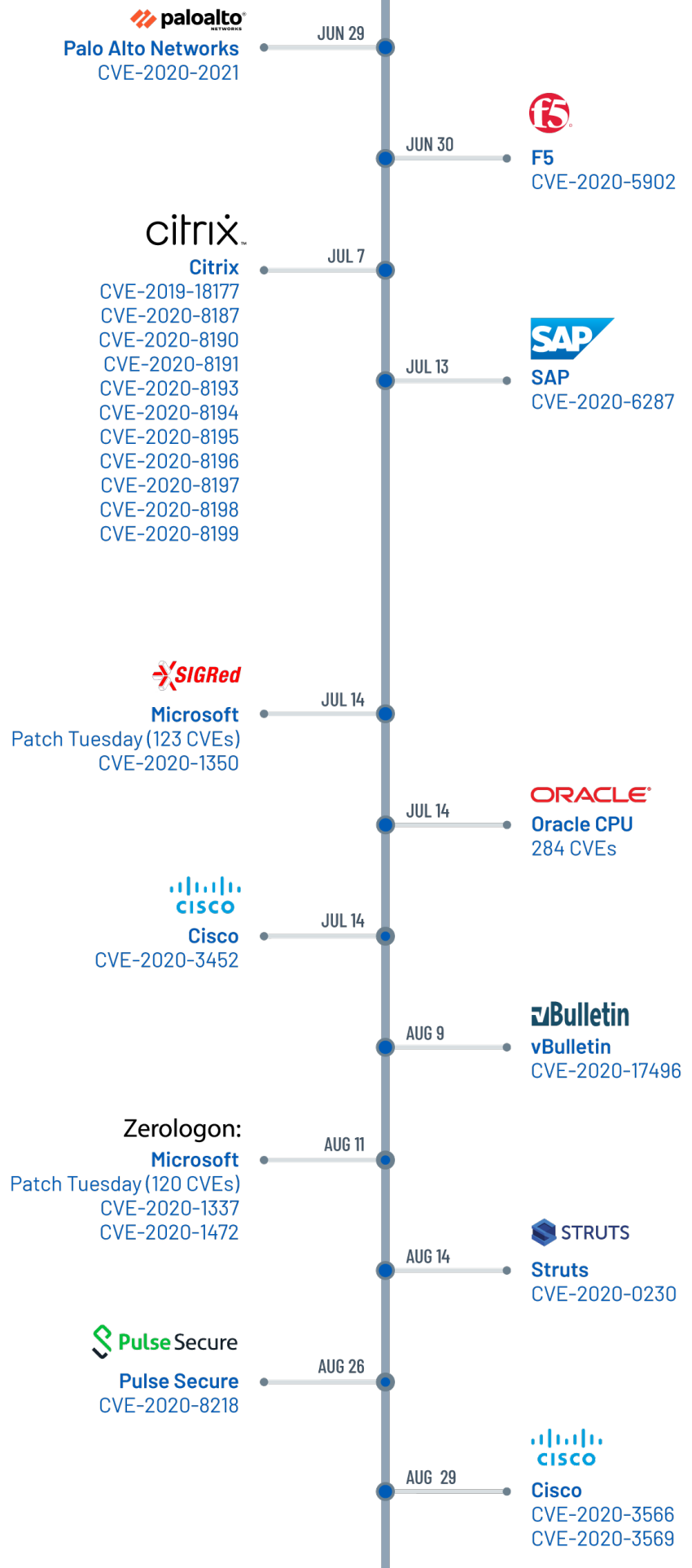
2020 Zero-Day Vulnerabilities by Software Type



Vulnerability Season

Prioritizing the patching of vulnerabilities is one of the many challenges cyber defenders face. Summer 2020 brought with it a slew of vulnerabilities rated CVSSv3 10.0, the maximum score possible, and considered critical for defenders. It's hard enough for defenders to prioritize remediation of vulnerabilities on a normal day, so being inundated with a flurry of activity during the summer was certainly overwhelming, as there were 547 vulnerabilities disclosed between June and August of 2020. Sean Gallagher, a threat researcher and former journalist, referred to this period of time as "CVE Season" in [a meme he shared on Twitter](#). Each new critical vulnerability disclosed over the span of two months pulled defenders' focus and made it difficult to keep pace. You can see in the timeline at the right the flurry of vulnerabilities defenders had to cope with from June to August.

THERE WERE
547
VULNERABILITIES
DISCLOSED
BETWEEN
JUNE AND
AUGUST OF 2020



COVID-19 and the Remote Workforce

It would be impossible to look back at 2020 and not discuss the COVID-19 pandemic. The emergence of the novel coronavirus in late 2019 triggered a swift and worldwide shift to remote work in an attempt to keep businesses running in the face of widespread lockdowns. Security and IT teams were tasked with securing this [expanded cyberattack surface](#), leveraging a variety of new applications to deliver a smooth transition and preparing for a barrage of threats targeting these newly remote employees.

The shift to a remote, distributed workforce has led to a higher volume of critical and confidential information being transmitted electronically, resulting in email servers becoming a prime target for threat actors. Two vulnerabilities in particular, [CVE-2020-0688](#), a validation key vulnerability in the Microsoft Exchange Control Panel, and [CVE-2019-10149](#), a remote code execution (RCE) [vulnerability in Exim](#), are favored by threat actors, as evidenced by their inclusion in an advisory from the U.S. government for the [top vulnerabilities targeted by state-sponsored actors](#). While patching email servers should be a priority to prevent exploitation and protect confidential information, educating staff on email best practices and raising security awareness in areas such as phishing should also be a top priority.

The increase in remote working has further consequences for IT administrators trying to implement and secure remote infrastructure, while also maintaining existing systems remotely. These workplace changes placed particular emphasis on three key areas:

- **Remote desktop protocol:**
The rush to remote work meant organizations had to lean heavily on RDP, a proprietary Windows protocol used to remotely access Windows servers and workstations in order to perform day-to-day tasks.
- **New apps on the block:**
The widespread lockdowns and travel restrictions thrust videoconferencing and collaboration tools into the spotlight at unprecedented speed and scale, giving attackers several juicy targets.
- **Malware and phishing scams:**
Historically, major events such as natural disasters allowed cybercriminals to capitalize on a crisis in a particular part of the world; for cybercriminals, COVID-19 provided a once-in-a-century opportunity to exploit fears on a global scale.

We explore each of these further in the subsections below.

**THE SHIFT TO
A DISTRIBUTED
WORKFORCE
HAS RESULTED IN
EMAIL SERVERS
BECOMING A
PRIME TARGET
FOR THREAT
ACTORS.**

THE ATTACK SURFACE FOR RDP IS VAST AND GROWING EXPONENTIALLY

Remote Desktop Protocol

RDP is included in each Windows operating system release. Although it is disabled by default, the ubiquity and convenience of RDP leads many organizations to utilize it to enable [Windows Remote Desktop Services](#). But RDP is not without its flaws, such as vulnerabilities and poor implementation.

The attack surface for RDP is vast and growing exponentially, accelerated by the increase in remote working. According to Shodan, a search engine for internet-connected devices, there are over [four and a half million internet-facing systems](#) with the Remote Desktop TCP port 3389 open. RDP also remains one of the most popular attack vectors for ransomware groups such as Sodinokibi, Maze and Phobos according to a [report from Coveware](#). In 2020, the FBI [issued a private industry notification to K-12 schools](#) in the United States that warned against ransomware attacks targeting vulnerable RDP systems, deployed as part of the shift to distance learning. This notification is one of several alerts the FBI has issued for RDP, from the more generalized [malicious activity perpetrated through the protocol](#) (2018) to its favored status among ransomware groups as a [key entry point for "high-impact ransomware attacks"](#) (2019).

For ransomware groups, there are a few different ways to breach RDP systems. The primary method is through brute-force. Ransomware gangs will try a number of different username and password combinations, including commonly used credentials, to see if they can gain access into the system. Ransomware gangs may also look to purchase stolen RDP credentials from underground markets. If brute force and stolen credentials aren't an option, attackers may try to exploit vulnerabilities in RDP. Below are four RDP vulnerability "collections" we believe are worth addressing based on publicly available proof-of-concept code as well as the potential impact to organizations from the exploitation of these flaws (more details on each can be found in Section 3):

1. [CVE-2019-0708](#), dubbed "BlueKeep," a pre-authentication RCE vulnerability in the way that incoming RDP requests are handled.
2. [CVE-2019-1181](#), [CVE-2019-1182](#), [CVE-2019-1222](#), and [CVE-2019-1226](#), collectively named "DejaBlue" by the research community because of the "deja vu" like feeling when comparing these vulnerabilities to BlueKeep.
3. [CVE-2019-1223](#), a Denial of Service (DoS) vulnerability
4. [CVE-2019-1224](#) and [CVE-2019-1225](#), a pair of information disclosure vulnerabilities.

Given the numerous and critical security risks around RDP, it's best to leave the protocol disabled. If it's necessary for business operations, organizations should take appropriate steps to secure it from these types of attacks. Apply patches in a timely manner, use strong passwords and configure the appropriate firewall rules and account lockout policy to restrict access and thwart credential stuffing attacks.

New Apps on the Block

After years of companies putting considerable effort into defending the perimeter and securing internal assets, the near-overnight change to remote work forced them to implement new applications such as virtual meeting software and Voice over Internet Protocol (VoIP) tools. In the rush to spin up these solutions, some organizations may have had no choice but to prioritize functionality over security. Below we highlight some primary areas of concern with such applications; more details on these vulnerabilities can be found in Section 3:



Zoom

Throughout 2020, Zoom faced scrutiny for privacy and data collection practices as the number of users on the platform increased at breakneck speed, exceeding its total monthly active users for calendar year 2019 [in just the first half of 2020](#).



Microsoft Teams

Capitalizing on the popularity of the Microsoft ecosystem, malicious actors set their sights on end-users via phishing attempts disguised as Microsoft Teams notifications in order to steal Office 365 credentials.



Cisco Webex

In similar attacks as those seen against Microsoft Teams, [the Cofense Phishing Defense Center published a blog post](#) in April regarding phishing emails posing as an alert for a critical security update to Webex. The phishing email even included a link to a legitimate security advisory from Cisco for [CVE-2016-9223](#). While phishing attacks such as these are a tried and true method for threat actors, researchers and attackers alike continue to hunt for vulnerabilities to exploit in Cisco products.



VoIP

VoIP technology has immensely eased the transition to remote work. Yet, as anyone in the security industry can attest, if a device is accessible over the network, it poses a security risk. Tenable Research found a stack-based buffer overflow vulnerability in Cisco Wireless IP phones that could be exploited by a remote, unauthenticated attacker using a simple [HTTP request](#). The findings highlight how a simple IP phone could be used as an entry point to a network by a determined attacker. The research also underscores the importance of patching and securing these devices.



COVID-19 Phishing and Malware Campaigns

While initial reports of COVID-19 first emerged in December 2019, it wasn't until the end of January 2020 that we began to see reports of COVID-19 becoming a lure used by cybercriminals. According to [a recent OpenText report](#), one out of four Americans say they received a COVID-19 related phishing email in 2020. By the first two weeks of April, [41% of organizations had experienced at least one business-impacting cyberattack](#) resulting from COVID-19 malware or phishing schemes.

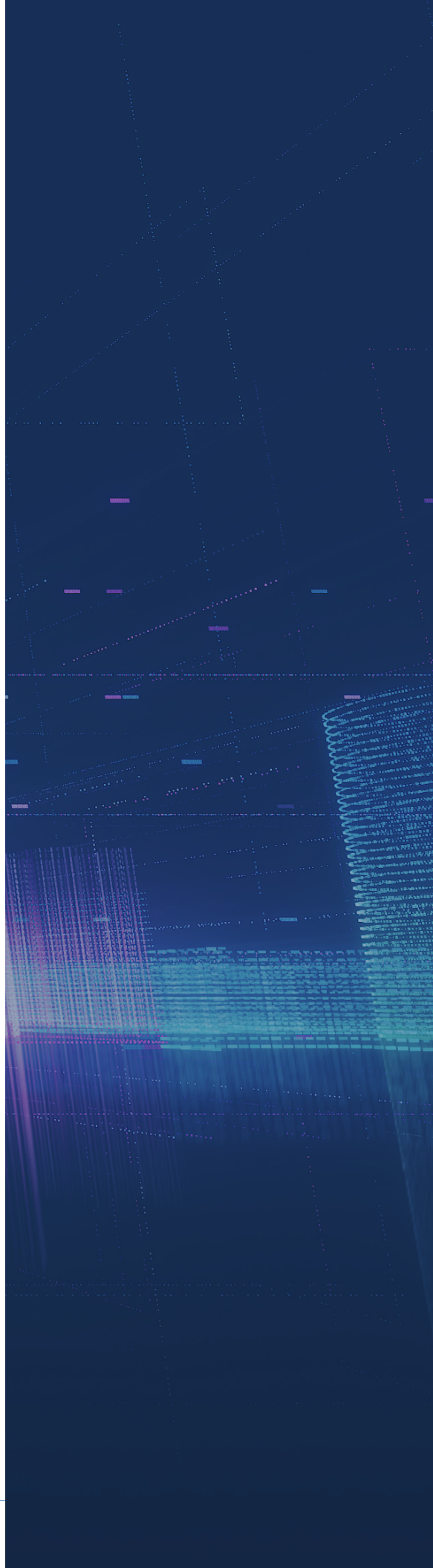
Below are four types of trojans or malware that were particularly attractive to scammers in 2020:

1. **Emotet**, a prolific banking trojan that has been used to perpetrate some of the biggest ransomware attacks
2. The **AZORult** trojan, which utilizes an exploit for [CVE-2017-11882](#), one of the most tried and true vulnerabilities used as part of malicious emails
3. The **Nanocore** remote access trojan, which gives attackers access to keystrokes and webcam feeds, as well as the ability to download and execute files
4. **Trickbot**, like Emotet, is a banking trojan that has become a lightning rod for ransomware gangs, often distributed as part of malicious emails and serving as an entry point into targeted networks

While most of the above examples were perpetrated via emails with malicious attachments, COVID-19 phishing attacks have also been prominent since the pandemic began. The examples below highlight just two of the ways attackers are exploiting the pandemic:

- In February, researchers at Kaspersky [shared details regarding a phishing campaign](#) claiming to be from the U.S. Centers for Disease Control and Prevention (CDC). The email includes a link reportedly to the CDC's official website. However, the link actually redirects users to a fake Microsoft Outlook phishing page in order to steal email credentials from unsuspecting users.
- In August, CISA [published an advisory](#) related to a phishing scheme impersonating the Small Business Administration's (SBA) COVID-19 loan relief program that [was announced earlier this year](#). The SBA program was designed to enable businesses struggling during COVID-19 to seek out debt relief, and apply for loans.

As long as the pandemic persists across the globe, it will remain a valuable lure for cybercriminals.



SECTION 2

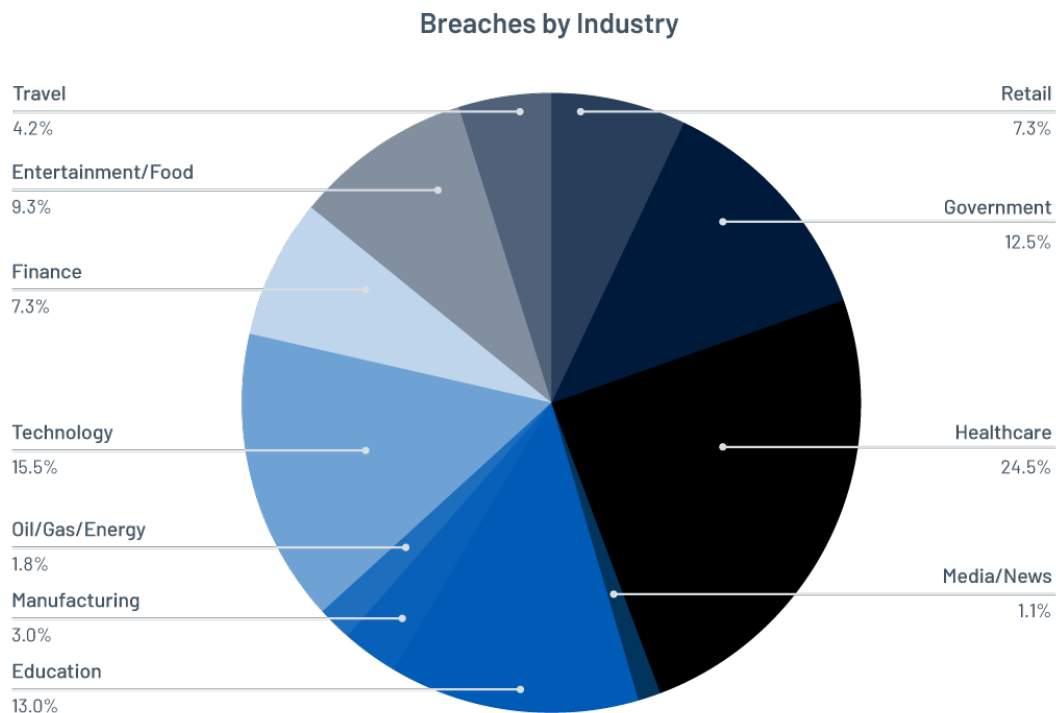
An Overview of the 2020 Threat Landscape

We would be remiss to discuss breaches in 2020 without first addressing the major incident that occurred right as everyone was preparing to wind down for the year. On December 13, news began to spread of a major breach at U.S. government agencies. Disclosures revealed that a backdoor had been introduced in the SolarWinds Orion Platform as part of its software builds for several months, and leveraged to infiltrate government agencies and private companies around the world.

The full extent of the SolarWinds breach won't be known until well into 2021, as more information is revealed about affected products and enterprises that were targeted. (The latest tally is 18,000 customers that downloaded the compromised software update.)

For the purposes of this report, we analyzed public breach disclosures from January to October 2020 to identify trends in breach data. In the first 10 months of 2020, there were 730 breach events resulting in over 22 billion records exposed. We split the data among 11 industry categories to get a broad picture of which sectors were most affected.

As the chart below indicates, healthcare and education accounted for the largest share of data breaches analyzed (25% and 13%, respectively). Healthcare breaches alone accounted for nearly 8 million records exposed. Government (12.5%) and technology (15.5%) were also frequent targets.



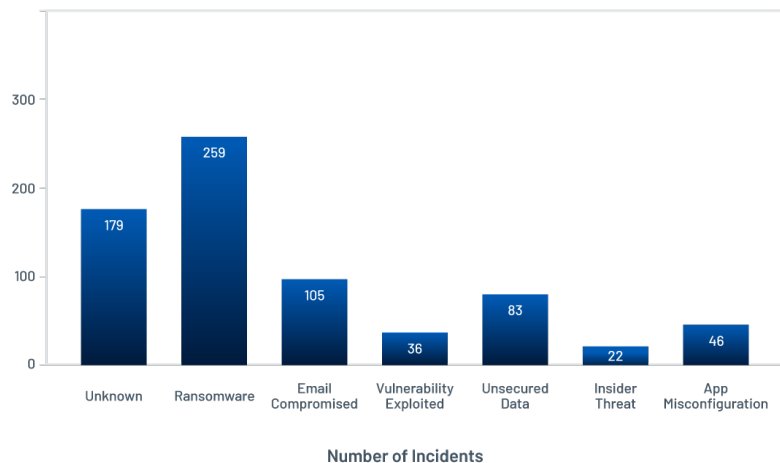
HEALTHCARE AND EDUCATION ACCOUNTED FOR THE LARGEST SHARE OF DATA BREACHES ANALYZED

After poring through the breach data, analyzing the root causes and organizing the results, we found some unexpected conclusions. While we anticipated some breach data would not include a root cause for the incident, we were not expecting to see nearly a quarter (24.5%) of cases fall into this category (as the chart to the right indicates).

While this finding may indicate a concerning gap in awareness of key threats, there is a silver lining: Organizations are reporting breaches early in their process, ensuring that affected individuals are aware of the incident and provided with tools to monitor for sensitive information leaks. At a time when dozens of unsecured data buckets and servers have leaked sensitive data, and ransomware continues to cripple networks across the world, our hope is that bringing these insights to the forefront will help companies understand the need for a strong data protection strategy.

For organizations around the world, data breaches are a costly and growing issue. While our analysis in this report does not attempt to examine this, researchers at IBM Security [estimated the global average cost](#) of a data breach at \$3.86 million. There's no doubt that data breaches will continue to trend upwards, not only in the number of breaches, but also in the number of records exposed.

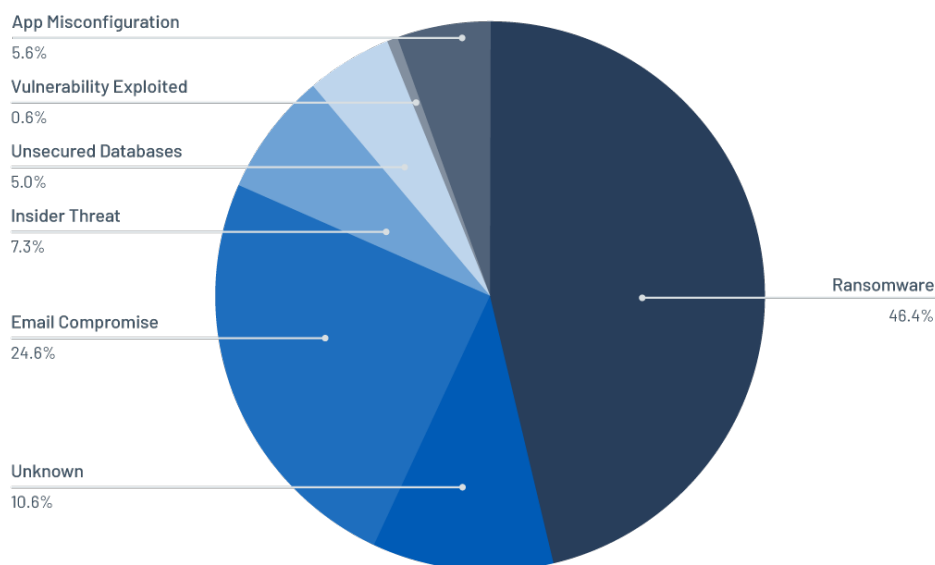
Root Cause




Ransomware remains a prominent root cause of healthcare breaches

Given the prevalence of breaches in the healthcare sector this year, we conducted a further root cause analysis and found that over 46% of the breaches in the sector were caused by ransomware attacks. As the chart below shows, other leading causes of breaches in healthcare included email compromise (24.6%), insider threats (7.3%) and application misconfiguration (5.6%).

Root Cause of Healthcare Breaches





Although ransomware loomed large for healthcare organizations in 2020, no industry sector is immune to its threat. Two of the foremost vulnerabilities leveraged by ransomware groups include a pair of VPN vulnerabilities found in the Citrix ADC controller, affecting Gateway hosts ([CVE-2019-19781](#)) and Pulse Connect Secure ([CVE-2019-11510](#)). These vulnerabilities, which we detail in Section 3, are a linchpin for nation-state threat actors, average cybercriminals and ransomware gangs looking to gain an initial foothold into any type of organization.

Unpatched vulnerabilities represent lucrative opportunities for bad actors. Researchers at Sophos speculate that the NetWalker ransomware group – which made a name for itself throughout 2020 through its successful breaches – targets vulnerabilities in “widely used, outdated server software,” citing Apache Tomcat and Oracle WebLogic as examples. (Both applications received patches for critical severity vulnerabilities in 2020.) In addition to exploiting these vulnerabilities, Sophos believes that NetWalker may target weak RDP passwords.

U.S. government issues alerts on VPN vulnerabilities and foreign threat actors targeting unpatched vulnerabilities

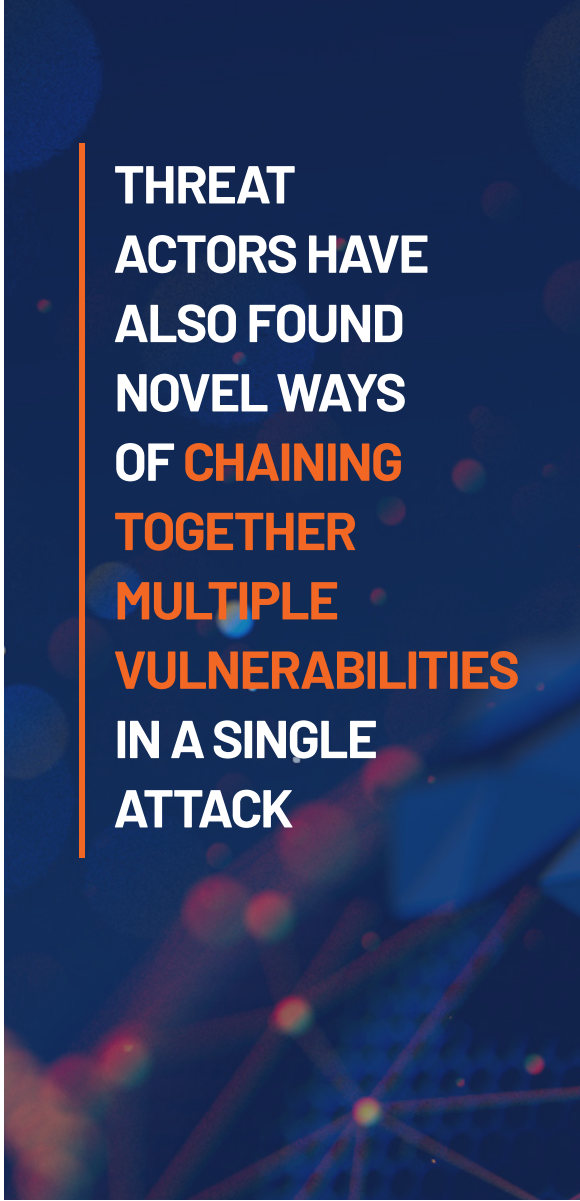
The [SolarWinds advisory](#) in mid-December may have been the most alarming of the alerts issued in 2020 by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), but it was hardly the only one. CISA and other government entities, including the Federal Bureau of Investigations (FBI) and the National Security Agency (NSA), issued several advisories regarding malicious activity from foreign threat actors. A few notable themes from these alerts include:

- **Enterprise-level systems are in the crosshairs:** The attacks on SolarWinds, F5, Cisco, VMWare and various VPN services all targeted systems that potentially offer broad and prospective means of access into large organizations and could open the door to extensive lateral movement.
- **Secure Socket Layer VPN vulnerabilities are “routinely exploited” in 2020:** In May 2020, CISA [published an alert](#) detailing the Top 10 Routinely Exploited Vulnerabilities from 2016 through 2019. In this alert, CISA warned that “malicious cyber actors” had set their sights on two VPN vulnerabilities, which were CVE-2019-19781 in Citrix and CVE-2019-11510 in Pulse Secure. These vulnerabilities have also been highlighted by U.S. government agencies when discussing advanced persistent threat group activity as part of multiple alerts released in October 2020

- **Threat actors are leveraging unpatched vulnerabilities as part of exploit chains:** In September, CISA published back-to-back advisories highlighting the increasing use of unpatched vulnerabilities in the toolkits of [Chinese](#) and [Iranian](#) threat actors, including the preferred usage of the three SSL VPN vulnerabilities we cover in Section 1. One month later, the NSA published an advisory of its own highlighting the Top 25 vulnerabilities used by Chinese state-sponsored threat actors, which highlight a plethora of unpatched vulnerabilities. Threat actors have also found novel ways of leveraging multiple vulnerabilities in a single attack. On October 9, CISA and the FBI issued a joint advisory that a foreign threat actor was exploiting “multiple legacy vulnerabilities” in an exploit chain with CVE-2020-1472, a critical elevation of privilege vulnerability in Windows Netlogon dubbed “ZeroLogon.” The legacy vulnerabilities mentioned in the alert include the three SSL VPN vulnerabilities we highlighted in Section 1, along with two other vulnerabilities, CVE-2020-5902 (F5 BIG-IP) and CVE-2020-1472 (Netlogon). The other legacy vulnerabilities leveraged by this threat actor included:

- [CVE-2020-1631](#), a local file inclusion vulnerability in Juniper’s Junos OS HTTP/HTTPS service;
- [CVE-2020-2021](#), an authentication bypass vulnerability in the Security Assertion Markup Language or SAML authentication in PAN-OS; and
- [CVE-2020-15505](#), an RCE vulnerability in MobileIron’s Core and Connector.

When left unpatched, these vulnerabilities are primarily used to gain initial access into a target network. From there, the attackers can chain together multiple legacy vulnerabilities with ZeroLogon in order to elevate privileges by granting themselves the ability to reset the password for and gain access to domain controllers within the network.



THREAT ACTORS HAVE ALSO FOUND NOVEL WAYS OF CHAINING TOGETHER MULTIPLE VULNERABILITIES IN A SINGLE ATTACK



SEP 14

CISA Alert
(AA20-258A)

SEP 15

CISA Alert
(AA20-259A)

OCT 9

CISA Alert
(AA20-283A)

OCT 20

NSA Advisory
U/00/179811-20

OCT 22

CISA Alert
(AA20-296A)

DEC 17

SolarWinds
(AA20-352A)

SECTION 3

A Closer Look at the Key Vulnerabilities in 2020

The checklist below, organized by vendors, provides details on the year's most significant vulnerabilities with additional insights on how they're being exploited.



Zero-day



Noteworthy



Exploited in
the Wild



Top 5



CVE-2020-1938: APACHE TOMCAT AJP FILE READ / INCLUSION VULNERABILITY ("GHOSTCAT")



In February, researchers at Chaitin Tech [disclosed a critical vulnerability in Apache Tomcat](#) identified as [CVE-2020-1938](#). Dubbed "Ghostcat," the researchers discovered a file read/inclusion vulnerability in the Apache JServ Protocol connector. This connector is part of the default configuration and can be configured by accessing it on HTTP port 8009. The vulnerability could be exploited by an unauthenticated, remote attacker allowing them to read web application files from a vulnerable server. The severity of this flaw increases on servers that allow for file uploads, which could allow the attacker to upload a malicious JavaServer Page file in order to gain remote code execution (RCE). There are currently over [28 repositories on GitHub](#) that host proofs-of-concept (PoCs) for Ghostcat.

CVE-2019-0230: APACHE STRUTS FORCED DOUBLE OBJECT-GRAPH NAVIGATION LANGUAGE (OGNL) EVALUATION VULNERABILITY

On August 14, Apache Struts [published a security bulletin \(S2-059\)](#) to address [CVE-2019-0230](#), a forced double object-graph navigation language (OGNL) evaluation vulnerability in Apache Struts version 2.0.0 through 2.5.20. It received a CVSSv3 score of 9.8. The vulnerability exists in the way Apache Struts tries to evaluate raw user input inside of tag attributes. In order to exploit the vulnerability, an attacker would need to inject malicious OGNL expressions into an attribute that is used within an OGNL expression. Successful exploitation of this vulnerability could lead to remote code execution. Despite having mitigations to address potential injected expressions, Apache Struts says that versions 2.5.22 and prior "left an attack vector open" which was addressed as part of the updates in the [S2-059 security bulletin](#). Apache Struts vulnerabilities often evoke memories of [CVE-2017-5638](#), a critical RCE vulnerability in Apache Struts 2 that led to the [Equifax breach](#) in 2017, which is considered one of the most notable breaches in recent history. Despite the specter of CVE-2017-5638, which was rated as a critical severity, CVE-2019-0230 was rated with an important severity, due to its limited impact.



CVE-2020-9818, CVE-2020-9819: IOS MAIL APP VULNERABILITIES



Since disclosure policies vary by vendor, some zero-day vulnerabilities may be considered more controversial, with researchers, vendors and the broader community engaging in heated debate. This was the case with a pair of Apple iOS zero-day vulnerabilities, identified as [CVE-2020-9818](#) and [CVE-2020-9819](#), an out-of-bounds write flaw and a heap overflow flaw in the iOS Mail App, both of which were reportedly [exploited in the wild](#).

- On April 20, ZecOps researchers published a [blog post](#) regarding their discovery. On iOS 13, the heap overflow was reportedly a zero-click vulnerability, meaning it could be triggered without interaction. However, on iOS 12, the heap overflow first required a user to click on a malicious email, and the out-of-bounds write vulnerability required the chaining of another vulnerability in order to trigger it remotely. Both vulnerabilities could be exploited via zero-click on iOS 12, but required the threat actor to gain control of the mail server. ZecOps noted it first observed attacks exploiting these vulnerabilities against devices running iOS 11.2.2 as early as January 2018. ZecOps also believes these vulnerabilities have been present since iOS 6, which was released back in September 2012.
- Apple countered ZecOps' claims in a [statement to Mark Gurman](#), Bloomberg's Apple correspondent, noting that these vulnerabilities by themselves are "insufficient to bypass iPhone and iPad security protections, and we have no evidence they were used against customers." ZecOps subsequently updated its blog to maintain that it observed "triggers in the wild for this vulnerability on a few organizations," and that it plans to "release more information and PoCs once a patch is available."

CVE-2020-27930, CVE-2020-27932, CVE-2020-27950: APPLE IOS AND IPAD OS VULNERABILITIES



On November 5, Apple released security updates for [macOS](#), iOS and iPad OS [[1](#), [2](#)], and watchOS [[1](#), [2](#), [3](#)], which included fixes for three zero-day vulnerabilities exploited in the wild. The vulnerabilities, identified as [CVE-2020-27930](#), [CVE-2020-27932](#) and [CVE-2020-27950](#), were discovered by Google's Project Zero team and [highlighted in a tweet](#) by technical lead Ben Hawkes.

- CVE-2020-2793 is a memory corruption vulnerability in the FontParser component due to the manner in which it processes font files; a maliciously crafted font file could lead to memory corruption, potentially resulting in an RCE attack.
- CVE-2020-2793 is a type confusion vulnerability in the kernel that could allow the execution of arbitrary code with kernel privileges and potentially allow malware to bypass security measures.
- CVE-2020-27950 is a memory initialization vulnerability that may be used to disclose kernel memory, which could contain sensitive and potentially useful information to an attacker, such as memory addresses and encryption keys.

This update includes the second font library-related zero-day vulnerability disclosed by Google's Project Zero team as being exploited in the wild, surfacing less than three weeks after CVE-2020-15999 was disclosed. Both font vulnerabilities may be related, as [suggested in a tweet](#) by Shane Huntley, the director of Google's Threat Analysis Group (TAG), who responded that these Apple bugs included "targeted exploitation in the wild similar to the other recently reported 0days."



Cisco Webex Vulnerabilities

The videoconferencing platform features multiple versions of Webex, including Webex Meetings, Webex Teams, Training Center and more. Because Cisco is such a popular vendor in the IT industry due to its wide variety of products, the company is no stranger to receiving vulnerability reports for its products. The table below contains some notable vulnerabilities within the Webex family of products that were disclosed in 2020:

CVE	Affected Devices	Vulnerability Type	CVSSv3
CVE-2020-3573 CVE-2020-3603 CVE-2020-3604	Cisco Webex Network Recording Player and Cisco Webex Player	Arbitrary Code Execution	7.8
CVE-2020-3128 CVE-2020-3127	Cisco Webex Network Recording Player and Cisco Webex Player	Arbitrary Code Execution	7.8
CVE-2020-3361	Cisco Webex Meetings and Cisco Webex Meetings Server	Unauthorized Access	9.8
CVE-2020-3263	Cisco Webex Meetings	Arbitrary Code Execution	7.5
CVE-2020-3342	Cisco Webex Meetings	Arbitrary Code Execution	8.8
CVE-2020-3194	Cisco Webex Network Recording Player and Cisco Webex Player	Arbitrary Code Execution	7.8
CVE-2020-3535	Cisco Webex Teams	DLL Hijacking	8.4

CVE-2020-3161: CISCO IP PHONES WEB SERVER REMOTE CODE EXECUTION AND DENIAL OF SERVICE VULNERABILITY

Voice over Internet Protocol (VoIP) technology has existed in various forms for many years. For businesses that rely on making and receiving phone calls, such as support centers, VoIP technology has immensely eased the transition to remote work. But as anyone in the security industry knows, if a device is accessible over the network, it poses a security risk. At Tenable Research, we conducted an investigation into Cisco Wireless IP Phones, and found a stack-based buffer overflow vulnerability that could be exploited by a remote, unauthenticated attacker using a simple [HTTP request](#). These findings were highlighted in [Tenable Research Advisory TRA-2020-24](#) and the vulnerability, identified as [CVE-2020-3161](#), was responsibly disclosed to Cisco. It received a critical CVSSv3 score of 9.8. The research reveals how a simple IP phone could be used as an entry point to a network by a determined attacker, underscoring the importance of patching and securing these vital devices.



In February, researchers at Armis Security disclosed five vulnerabilities in the proprietary Cisco Discovery Protocol (CDP). The protocol is designed to enable Cisco devices to discover and communicate with one another on a network. The five vulnerabilities are collectively referred to as **CDPwn** and result from an improper validation of messages sent through CDP. An attacker would need to be in the same broadcast domain as a vulnerable device to exploit one of these flaws. Armis says that the vulnerabilities “affect tens of million devices,” including Cisco switches, routers, IP cameras, firewalls, and IP phones. For several months, there were no indications that any of these vulnerabilities had been exploited in the wild. However, in October, the National Security Agency published a list of top vulnerabilities exploited by a nation-state actor from China, which included CVE-2020-3118, one of the CDPwn vulnerabilities.

CVE	Affected Devices	CVSSv3
CVE-2020-3110	Cisco Video Surveillance 800 Series IP Cameras	8.8
CVE-2020-3111	Cisco IP Phone	8.8
CVE-2020-3118	Cisco IOS XR	8.8
CVE-2020-3119	Cisco NX-OS	8.8
CVE-2020-3120	Cisco FXOS, IOS XR, NX-OS	7.4

CVE-2020-3566, CVE-2020-3569: CISCO IOS XR SOFTWARE DENIAL OF SERVICE VULNERABILITIES



On August 29, Cisco [published an advisory](#) for a pair of zero-day denial of service (DoS) vulnerabilities in its Cisco IOS XR Software, identified as [CVE-2020-3566](#) and [CVE-2020-3569](#). The advisory was released in response to active exploitation, which the Cisco Product Security Incident Response Team became aware of on August 28. The vulnerabilities exist in the Distance Vector Multicast Routing Protocol feature of Cisco IOS XR Software, but stemmed from the vulnerable devices incorrectly implementing management for Internet Group Management Protocol packets. Successful exploitation would result in resource exhaustion leading to instability in running processes, which could potentially cripple a network by impacting internal and external routing protocols.

CVE-2020-3452: CISCO ADAPTIVE SECURITY APPLIANCE AND FIREPOWER THREAT DEFENSE DIRECTORY TRAVERSAL VULNERABILITY



On July 22, Cisco published an advisory for CVE-2020-3452, a read-only directory traversal vulnerability in Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense software. This vulnerability received a CVSSv3 score of 7.5. The vulnerability is present when the devices are configured to run WebVPN or AnyConnect. An attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable system that contains a directory traversal character sequence (e.g. “../”). PoC exploits for this vulnerability were published by Ahmed Aboul-Ela, one of the researchers credited with discovering the vulnerability. This vulnerability was also credited to Mikhail Klyuchnikov of Positive Technologies. Klyuchnikov has been credited with finding other directory traversal vulnerabilities, including CVE-2019-19781 in Citrix and CVE-2020-5902 in F5 BIG-IP. Because CVE-2020-3452 is a read-only vulnerability, it does limit some of its impact. However, Klyuchnikov called the vulnerability “highly dangerous” because an attacker would be able to gain access to RamFS, the file system that stores data in RAM. This means an attacker would be able to read configuration files from WebVPN for Cisco ASA users, including bookmarks, cookies, web content and HTTP URL addresses. Cisco notes in its advisory that it is aware of PoC code for this vulnerability as well as active exploitation in the wild.

CVE-2019-19781: CITRIX APPLICATION DELIVERY CONTROLLER (ADC) AND GATEWAY



In December 2019, Citrix [published a support article](#) for a critical vulnerability in its Application Delivery Controller (ADC) and Gateway, formerly known as NetScaler ADC and NetScaler Gateway. The vulnerability, identified as [CVE-2019-19781](#), is a directory traversal vulnerability in the ADC and Gateway products. An unauthenticated, remote attacker could exploit the vulnerability by sending a specially crafted request containing a directory traversal string to the vulnerable Citrix endpoint. Successful exploitation would grant an attacker the ability to execute arbitrary code. Citrix did not initially provide a patch for CVE-2019-19781 when it announced the vulnerability in December 2019, but ultimately patched these vulnerabilities in January 2020. The directory traversal allows an attacker to access Perl scripts located within the /vpns/ path on Citrix appliances, which can result in a limited file write on the vulnerable host. One of the scripts in the /vpns/ path used an undocumented feature in the Perl Template Toolkit, which [according to Rio Sherri](#), a senior security consultant at MDSec, allows for “arbitrary command execution when processing a crafted directive.” This became the focus of exploitation. On January 3, 2020, researchers at the SANS Internet Storm Center [tweeted](#) that they observed exploitation attempts against one of their Citrix ADC/Gateway honeypots. On June 7, SANS ISC [shared more details](#) about the exploitation attempts it observed against its honeypots. As more researchers publicized information surrounding the flaw, it was only a matter of time before PoC code and exploit scripts were uploaded to GitHub. Predictably, the availability of PoC and exploit scripts became a boon for cybercriminals.

11 VULNERABILITIES IN CITRIX APPLICATION DELIVERY CONTROLLER (ADC), GATEWAY AND SD-WAN WANOP



In early July, Citrix [published a support article addressing 11 vulnerabilities](#) patched across its Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP devices. These include information disclosure, elevation of privileges, cross-site scripting (both stored and reflected), DoS, code injection and authorization bypass vulnerabilities. Three of the vulnerabilities — all located in the Citrix management interface — have since been [actively exploited in the wild](#), including CVE-2020-8193, an authorization bypass vulnerability, as well as CVE-2020-8195 and CVE-2020-8196, two information disclosure vulnerabilities. The latter two are post-authentication vulnerabilities, meaning that an attacker would need to already have access to the device, or exploit the authorization bypass vulnerability, to retrieve sensitive device information, such as configuration files. This retrieval could also result in the exposure of password hashes that could be easy to crack using tools such as Hashcat. These Citrix-related vulnerabilities are garnering more attention because of CVE-2019-19781, a critical directory traversal vulnerability in Citrix ADC, Gateway, and SD-WAN WANOP devices, which was christened one of the [Top 10 Most Routinely Exploited Vulnerabilities](#) in 2020 by the Cybersecurity and Infrastructure Security Agency (CISA). Therefore, it comes as no surprise that a subset of these newly disclosed Citrix vulnerabilities, CVE-2020-8193, CVE-2020-8195 and CVE-2020-8196, were [featured in the NSA's advisory for Top 25 vulnerabilities](#) exploited by Chinese nation-state threat actors. The following is the list of vulnerabilities patched by Citrix as part of this release:

CVE	CVSSv3	CVE	CVSSv3
CVE-2019-18177	N/A	CVE-2020-8195	6.5
CVE-2020-8187	7.5	CVE-2020-8196	4.3
CVE-2020-8190	7.5	CVE-2020-8197	8.8
CVE-2020-8191	6.1	CVE-2020-8198	6.1
CVE-2020-8193	6.5	CVE-2020-8199	7.8
CVE-2020-8194	6.5		



CVE-2020-5902: F5 BIG-IP DIRECTORY TRAVERSAL VULNERABILITY



In late June, F5 [published a support article](#) for [CVE-2020-5902](#), a critical directory traversal vulnerability in the traffic management user interface (TMUI) of its BIG-IP product line, which includes a variety of software and hardware-based solutions that provide access control, application availability and security. To exploit the vulnerability, an unauthenticated, remote attacker could send a specially crafted request to a vulnerable BIG-IP device containing a directory traversal character sequence (e.g. "../") unlocking the ability to execute arbitrary system commands, create or delete files or disable services on the vulnerable host. Security researchers latched on to this vulnerability, with one researcher calling this "one of the most impactful vulnerabilities" they had seen in over 20 years in the information security space. Soon after PoC code was published for this vulnerability, attackers seized the opportunity to exploit publicly accessible BIG-IP systems.



CVE-2018-13379: FORTINET FORTIOS SSL VPN WEB PORTAL INFORMATION DISCLOSURE



In May 2019, Fortinet published an advisory for [CVE-2018-13379](#), a pre-authentication information disclosure vulnerability in its FortiOS Secure Socket Layer Virtual Private Network (SSL VPN). Details about this vulnerability and several others in the FortiOS SSL VPN were shared by DEVCORE researchers Meh Chang and Orange Tsai [in a blog post](#) in August 2019. CVE-2018-13379 is also known as an arbitrary file read vulnerability, which allows attackers to read the contents of a session file that contains a username and plaintext password. This is achieved by sending a specially crafted request to the vulnerable FortiOS SSL VPN. Attackers could then leverage this information to authenticate to the SSL VPN, before chaining CVE-2018-13379 with a separate FortiOS SSL VPN vulnerability, such as [CVE-2018-13383](#), a post authentication heap buffer overflow vulnerability, in order to get a shell on the system. CVE-2018-13379 is one of our Top 5 Vulnerabilities in 2020 because it has been a frequent favorite amongst cybercriminals. In August 2019, soon after a PoC became available for this vulnerability, attackers were quick to begin exploiting it in the wild. In 2020, it has been frequently cited in a number of U.S. Government Alerts from CISA and the NSA.



CVE-2020-6418: GOOGLE CHROME TYPE CONFUSION VULNERABILITY



On February 24, Google released a [stable channel update](#) for Google Chrome Desktop. The stable channel update is the official production-ready release of Google Chrome that contains fixes for bugs and security vulnerabilities. In this release, Google addressed multiple vulnerabilities, including one [reported as exploited in the wild](#). The flaw identified as [CVE-2020-6418](#) is a type confusion vulnerability in [V8](#), Google Chrome's JavaScript engine. The vulnerability was reported by Clément Lecigne, security engineer at Google's Threat Analysis Group (TAG), who was responsible for previously reporting [CVE-2019-5786](#), a Chrome zero-day that [was also targeted in the wild](#).

CVE-2020-15999: GOOGLE CHROME HEAP BUFFER OVERFLOW IN FREETYPE VULNERABILITY



On October 20, Google released another [stable channel update](#) for Chrome's Desktop release that included a fix for an [actively exploited zero-day vulnerability](#). The vulnerability, identified as [CVE-2020-15999](#), is a heap buffer overflow that exists in the "Load_SBit_Png" function of the FreeType 2 library used by Google Chrome. Exploitation of this vulnerability would require some form of social engineering to convince a victim to visit a malicious website containing a specially crafted font file.

CVE-2020-16009, CVE-2020-16010: GOOGLE CHROME AND CHROME FOR ANDROID VULNERABILITIES



On November 2, Google [released another stable channel](#) update for Google Chrome. This update addressed seven vulnerabilities, including [CVE-2020-16009](#), a zero-day vulnerability reportedly exploited in the wild. On the same day, Google also released a [Chrome for Android update](#) addressing [CVE-2020-16010](#), an actively exploited zero-day in Chrome for Android. The Google Chrome for Desktop vulnerability, CVE-2020-16009, exists due to the inappropriate implementation of the V8 JavaScript engine, the second V8 Chrome zero-day targeted in 2020 (the first being CVE-2020-6418). To exploit the vulnerability, an attacker would need to create a specially crafted HTML page and convince a victim to visit it, resulting in system compromise. Further details were not disclosed in accordance with Google's policy, which states that "access to bug details and links may be kept restricted until a majority of users are updated with a fix." The Android vulnerability, CVE-2020-16010, is a heap-based buffer overflow in the user interface component of Chrome that exists when it processes untrusted HTML content. Similar to CVE-2020-16009, an attacker would need to convince the victim to visit a specially crafted HTML page to exploit this vulnerability, which could result in a sandbox escape if the rendered process was compromised.

CVE-2020-16013, CVE-2020-16017: GOOGLE CHROME VULNERABILITIES



On November 11, Google once again released a [stable channel update](#) for Google Chrome which included fixes for two actively exploited zero-day vulnerabilities, identified as [CVE-2020-16013](#) and [CVE-2020-16017](#). CVE-2020-16013 is a vulnerability in the V8 JavaScript engine due to "inappropriate implementation." This marks the second Chrome zero-day reported in less than a month affecting the V8 engine, and the third one reported in 2020. CVE-2020-16017 is a use-after-free memory corruption bug in the [Site Isolation](#) component of Google Chrome. A vulnerability in this component is worth paying attention to, as it is responsible for enforcing same-origin policy and offers protection against vulnerabilities, such as the speculative side-channel attacks like Spectre and Meltdown. The disclosure of CVE-2020-16013 and CVE-2020-16017 rounds out the number of Chrome zero-days disclosed in less than a month to five. Tim Willis of Google's Project Zero team reflected on the impact of these disclosures [in a tweet](#), stating that Project Zero's "7-day disclosure policy needs a bit of work to consistently get the best results for user security," after his team reported nine zero-day vulnerabilities in 2020 following this process.

**THE DISCLOSURE OF CVE-2020-16013 AND CVE-2020-16017
ROUNDS OUT THE NUMBER OF CHROME ZERO-DAYS
DISCLOSED IN LESS THAN A MONTH TO FIVE**



Microsoft Teams



A popular video conferencing solution, Microsoft Teams became a high-value target for attackers this year. Capitalizing on the popularity of the Microsoft ecosystem, malicious actors set their sights on end-users via phishing attempts disguised as Microsoft Teams notifications in order to steal Office 365 credentials. [Details about these attacks](#) surfaced around the same time that CISA [published an alert](#) regarding Microsoft Office 365 security recommendations and best practices. Researchers at CyberArk also [identified a severe flaw](#) that could be exploited to exfiltrate sensitive information from users by simply opening a message containing a specially crafted GIF image. CyberArk disclosed the vulnerability to Microsoft, which subsequently released a patch, though it did not receive a CVE identifier. This wasn't the only Microsoft Teams vulnerability that Microsoft patched in 2020. As part of its November 2020 Patch Tuesday release, Microsoft patched [CVE-2020-17091](#), an unspecified RCE in Microsoft Teams, closing another flaw that could have been exploited by a local attacker. Additionally, security engineer Oskars Vegeris [disclosed a significant "zero-click" RCE in Teams](#) that was patched silently and did not receive a CVE identifier.

CVE-2020-0601: SPOOFING VULNERABILITY IN MICROSOFT CRYPTOAPI ("CURVEBALL")



On January 7, hours before the first Microsoft Patch Tuesday of 2020, the security community was ablaze with speculation about a severe vulnerability in Microsoft's Windows operating system (OS). Shortly after rumors and discussions began on social media, details emerged about [CVE-2020-0601](#), a spoofing vulnerability in a core cryptographic module in Microsoft Windows (crypt32.dll). The vulnerability was discovered and reported to Microsoft by the NSA, which issued an [advisory](#) highlighting its severity. An attacker who successfully exploits this critical flaw would be able to deliver malicious code that appears signed and from a trusted entity, bypassing Windows' ability to verify cryptographic trust. Because this flaw resides in a core cryptographic module, Windows systems that remain unpatched are at risk from a wide range of attack vectors.

CVE-2020-17087: WINDOWS KERNEL ELEVATION OF PRIVILEGE VULNERABILITY



On October 30 Ben Hawkes, of Google's Project Zero team, [tweeted](#) that his team detected a Windows kernel bug being exploited alongside CVE-2020-15999. The vulnerability, identified as [CVE-2020-17087](#), is a "pool-based" buffer overflow in the `cn!CfgAdtpFormatPropertyBlock` function of the Windows Kernel Cryptography Driver (cng.sys) due to a 16-bit integer truncation. Microsoft decided not to publish an out-of-band (OOB) patch for this vulnerability, opting to follow its standard patch process and address it in the [November 2020 Patch Tuesday](#) release. The tweet by Hawkes also notes that the [chaining of CVE-2020-17087 with CVE-2020-15999](#) could allow an attacker to escape Google Chrome's sandbox, moving beyond the browser to target the underlying Windows system, potentially allowing for elevation of privileges and execution of arbitrary code.

CVE-2020-1472: ELEVATION OF PRIVILEGE VULNERABILITY IN NETLOGON (“ZEROLOGON”)



On August 11, Microsoft [published its Patch Tuesday release for August 2020](#), marking the seventh month in a row with over 100 CVEs being patched. One of the more noteworthy vulnerabilities patched in the August 2020 release included CVE-2020-1472, a critical vulnerability in Microsoft Windows Netlogon. At the time this vulnerability was patched in August, the full details about it were not known. However, a month later, researchers at Secura [published a whitepaper and blog post](#) about this vulnerability, which they dubbed “Zerologon,” along with a PoC exploit. The whitepaper details how an attacker could exploit the flaw to take over a domain controller, giving them complete control over a Windows domain. Following this publication, researchers began to investigate further. Dirk-Jan Mollema, a security researcher at Fox-IT, published a working exploit script to GitHub that made the exploitation of Zerologon easy and reliable. Zerologon would go on to be included as part of the [CISA Emergency Directive 20-04](#), which required the public sector to apply the patch for the vulnerability immediately. This decision was prescient as future U.S. government alerts highlighted the use of Zerologon in attacks perpetrated against the public sector by nation-state actors from China and Russia.

CVE-2020-1337: WINDOWS PRINT SPOOLER ELEVATION OF PRIVILEGE

As part of the August Patch Tuesday release, another critical elevation of privilege flaw was fixed by Microsoft, CVE-2020-1337. Successful exploitation would allow an attacker to arbitrarily write to the filesystem. The vulnerability, located within Windows Print Spooler, is actually a bypass of CVE-2020-1048, another elevation of privilege vulnerability that was dubbed “PrintDemon” by security researcher Alex Ionescu. It received a CVSSv3 score of 7.8 and a PoC was published shortly after the patch release.

RDP VULNERABILITIES FROM 2019 BECAME MORE VALUABLE AMID GLOBAL PANDEMIC



Microsoft’s Remote Desktop Protocol (RDP) implementations are particularly favored by enterprise users. RDP is used to connect to Windows machines, giving users the ability to interact with the systems as if they were in the same room as the machine itself. As businesses moved to remote operations in 2020, attackers continued to target the protocol, particularly in ransomware attacks. Renewed interest in RDP began in 2019 with [CVE-2019-0708](#), a critical pre-authentication RCE vulnerability in Remote Desktop Services, named “BlueKeep” by security researcher Kevin Beaumont. When developing patches for BlueKeep in May 2019, Microsoft took the unusual approach of including patches for Windows XP and Windows Server 2003, legacy versions of Windows that are no longer supported by Microsoft. Exploitation of BlueKeep requires the attacker to send a malicious request to the RDP service, which could result in the complete takeover of a vulnerable device. Despite the severity of the issue, initial exploitation observed in the wild was limited to [delivering cryptocurrency miners to vulnerable systems](#). In late 2020, we learned that an uncharacterized threat group known as UNC1945 had been [using BlueKeep as part of its reconnaissance efforts](#). Three months after BlueKeep was patched, Microsoft patched four pre-authentication RCE RDP vulnerabilities in the [August 2019 Patch Tuesday](#) update. These vulnerabilities, identified as [CVE-2019-1181](#), [CVE-2019-1182](#), [CVE-2019-1222](#) and [CVE-2019-1226](#), were dubbed “DejaBlue” by the research community. The August 2019 Patch Tuesday update included three additional RDP vulnerabilities: [CVE-2019-1223](#), a DoS vulnerability, along with [CVE-2019-1224](#) and [CVE-2019-1225](#), a pair of information disclosure vulnerabilities. Since the release of BlueKeep, it has been common for Patch Tuesday to include patches for RDP vulnerabilities; however, in the span of three months, all Windows OS variants were affected by at least one RDP RCE vulnerability.

CVE-2020-0688: MICROSOFT EXCHANGE SERVER VALIDATION KEY VULNERABILITY



In February, researchers at the Zero Day Initiative (ZDI), [published a blog post](#) regarding the disclosure of [a serious vulnerability in Microsoft Exchange Server](#) that was patched during [February's Patch Tuesday release](#). The flaw, identified as [CVE-2020-0688](#), is a validation key vulnerability due to the generation of static cryptographic keys. To exploit this vulnerability, an attacker would already need to be authenticated to a vulnerable Exchange Server. While this may seem like an impediment, [researchers identified open-source tools](#) that can overcome the authentication requirement, by scraping data from sources such as LinkedIn to gather information about employees and perform credential stuffing attacks. There are currently [16 PoCs for this vulnerability on GitHub](#). Soon after the vulnerability was disclosed, [reports began to emerge](#) that threat actors were utilizing the flaw in the wild.

CVE-2020-0796: MICROSOFT SERVER MESSAGE BLOCK V3 VULNERABILITY ("SMBGHOST")



In March, Microsoft [unintentionally disclosed a critical vulnerability in Microsoft Server Message Block v3 \(SMBv3\)](#) as part of its [March Patch Tuesday](#) release. The vulnerability was [eventually made public](#) and received its own [advisory page](#). Identified as [CVE-2020-0796](#), the flaw exists due to the way certain requests are handled by SMBv3. A remote, unauthenticated attacker could exploit the vulnerability against a vulnerable SMBv3 server by sending a specially crafted packet. To exploit the flaw on an SMBv3 client, the attacker would need to convince their victim to connect to a malicious SMBv3 server, likely using social engineering tactics. Exploitation through either method would result in remote code execution on the respective SMBv3 instance, be it server or client. Researchers have referred to this vulnerability as [EternalDarkness](#) and [SMBGhost](#). There are currently 75 PoCs available on GitHub for this vulnerability. Initially, many of the PoCs released led to a DoS condition or privilege escalation. However, in June, a [PoC exploit to achieve RCE](#) was released.

CVE-2020-0938, CVE-2020-1020 AND CVE-2020-1027: MULTIPLE ZERO-DAY VULNERABILITIES IN MICROSOFT'S APRIL 2020 PATCH TUESDAY



Microsoft's [April 2020 Patch Tuesday](#) addressed 113 CVEs, including patches for three zero-day vulnerabilities that were actively exploited in the wild. [CVE-2020-0938](#) and [CVE-2020-1020](#) are RCE vulnerabilities in the Windows Adobe Type Manager Library due to an improper handling of the Adobe Type 1 PostScript font format. These vulnerabilities were initially highlighted by Microsoft in [ADV200006](#), an OOB advisory published by Microsoft due to reports of active exploitation in the wild. [CVE-2020-1027](#), the third zero-day vulnerability, is a flaw in the Windows kernel that would allow for elevation of privileges due to improper handling of objects in memory. Initially, a fourth vulnerability, [CVE-2020-0968](#), a memory corruption flaw, was highlighted as exploited in the wild, but Microsoft [updated its exploit status](#) to clarify it had in fact not been.

CVE-2020-0986: WINDOWS KERNEL ELEVATION OF PRIVILEGE VULNERABILITY



On June 9, Microsoft's [June 2020 Patch Tuesday](#) addressed 129 vulnerabilities, including a single zero-day vulnerability that was exploited in the wild. The vulnerability, identified as [CVE-2020-0986](#), is a local privilege escalation vulnerability in `sp/wow64.exe` that exists because of how it handles the C++ library `memcpy` function. The vulnerability allows `memcpy` to send arbitrary parameters via a local procedure call to `sp/wow64.exe`. It leverages `memcpy` calls the same way as [CVE-2019-0880](#), which was patched in [Microsoft's July 2019 Patch Tuesday](#). Microsoft's [advisory for CVE-2020-0986](#) did not indicate that the vulnerability had been exploited in the wild, however, researchers at Kaspersky confirmed observation of active exploitation [as part of Operation Powerfall](#). A [Google Project Zero document](#) sheds light on this discrepancy: Microsoft was not initially aware of the confirmed exploit, and the company has a policy of not updating the "exploited" flag after an advisory is published.

CVE-2020-1350: WINDOWS DOMAIN NAME SYSTEM REMOTE CODE EXECUTION VULNERABILITY (“SIGRED”)



Microsoft’s [July Patch Tuesday release](#) marked the sixth month in a row that Microsoft released patches for over 100 CVEs. One of the most noteworthy vulnerabilities patched in this release was [CVE-2020-1350](#), an RCE vulnerability that results from how the Windows Domain Name System (DNS) Server parses requests. Dubbed “SigRed” by Check Point Research, the vulnerability received a CVSSv3 score of 10.0. Check Point Research believes this vulnerability has been present in DNS Server for 17 years, which means it affects Windows Server version 2003 through 2019. Microsoft noted this vulnerability is “wormable” which means that it could spread between vulnerable systems without any sort of user interaction. Microsoft took an important step to release patches for Windows Server 2008, which reached its end of life in January 2020, further emphasizing the severity of this vulnerability and the worry that the wormable potential could lead to an event similar to the [WannaCry](#) attacks in 2017.

CVE-2020-0674: INTERNET EXPLORER REMOTE CODE EXECUTION VULNERABILITY



On January 17, Microsoft released an [OOB advisory](#) (ADV200001) for [CVE-2020-0674](#), a zero-day RCE vulnerability in Internet Explorer. While an OOB advisory alone from Microsoft is enough to catch the attention of most IT administrators or security professionals, this one stood out given the company’s reports of [exploitation in the wild](#) and knowledge of “limited targeted attacks.” Microsoft’s advisory included mitigations but no accompanying patch, as the company decided to stand behind its Patch Tuesday process stating “this predictable schedule allows for partner quality assurance and IT planning.”

CVE-2020-1380: INTERNET EXPLORER SCRIPTING ENGINE MEMORY CORRUPTION VULNERABILITY



Microsoft’s [August 2020 Patch Tuesday](#) release addressed 120 vulnerabilities, including a patch for [CVE-2020-1380](#), the second vulnerability in Internet Explorer that was exploited in the wild this year. CVE-2020-1380 is an RCE vulnerability in Internet Explorer due to the way its scripting engine handles objects in memory. Successful exploitation of this vulnerability would likely require some form of social engineering. This includes convincing a victim to visit a maliciously crafted website that exploits the vulnerability or tricking a victim to open a specially crafted Microsoft Office document.

moz://a

CVE-2019-17026: MOZILLA FIREFOX TYPE CONFUSION VULNERABILITY



Zero-day vulnerabilities got an early start in 2020 when the Mozilla Foundation [released an advisory](#) on January 8 for [CVE-2019-17026](#), a type confusion vulnerability in Mozilla Firefox that was being [exploited in targeted attacks](#). The vulnerability was reported to Mozilla by researchers at Qihoo 360.



On April 3, the Mozilla Foundation released [advisories](#) for Mozilla Firefox and Mozilla Firefox Extended Support Release. The advisories addressed a pair of [critical zero-day use-after-free vulnerabilities](#), identified as [CVE-2020-6819](#) and [CVE-2020-6820](#). Mozilla noted for the second time this year that it is “aware of targeted attacks in the wild abusing this flaw.” Zero-day browser vulnerabilities have been a recurring trend and attractive target for threat actors throughout 2020. The vulnerabilities were credited to Javier Marco and Francisco Alonso, with Alonso noting in a since-removed tweet that “There is still lots of work to do and more details to be published (including other browsers)” indicating that these vulnerabilities impacted browsers other than Mozilla Firefox.



CALLSTRANGER



On June 8, [CVE-2020-12695](#), a server-side request forgery (SSRF) vulnerability in devices that utilize Universal Plug and Play (UPnP) protocol, was disclosed by Yunus Çadirci in an [advisory](#). Çadirci dubbed the vulnerability [CallStranger](#) given the ability to control the Callback header value in the UPnP SUBSCRIBE function. Çadirci’s advisory claims that “billions of UPnP devices on the local network and millions of UPnP devices on the Internet are exposed” as UPnP is used by [hundreds of vendors](#) spanning a multitude of devices. While this sounds like it could be devastating, the biggest potential risk from exploitation is data exfiltration or more likely use in distributed denial of service (DDoS) scenarios. While it doesn’t carry the same weight as an RCE vulnerability, this doesn’t mean it should be ignored. As the vulnerability resides at a protocol-level, the changes made within the UPnP protocol specification fell to the [Open Connectivity Foundation](#). Individual manufacturers implementing this protocol in their products would need to assess the protocol specifications and release patches for supported devices.



OPERATING SYSTEMS

BOOTHOLE



[CVE-2020-10713](#), known as BootHole, is a buffer overflow vulnerability in GRand Unified Bootloader version 2 (GRUB2). This is a piece of software for Windows and Linux, and the default boot loader for many *nix distributions which loads an OS into memory when a system boots up. The vulnerability exists as a result of how GRUB2 parses grub.cfg, a configuration file containing a list of installed kernels and bash-like code. An attacker that successfully modifies the grub.cfg file, which is not signed, would be able to bypass Secure Boot, giving them persistent exploitation after the system loads. The researchers at [Eclypsium responsible for its disclosure](#) dubbed the vulnerability “[BootHole](#)” due to its impact on the GRUB2 bootloader on devices using Secure Boot. In addition to assigning it a name, the researchers also created a humorous yet appropriate logo. With a catchy name and logo, and a broad list of affected operating systems with serious potential impact, why haven’t there been reports of widespread exploitation? The main caveat is that an attacker needs local access to a vulnerable device and elevated or administrator privileges to exploit BootHole. With local access already obtained, an attacker can likely leverage more practical attack vectors.

CVE-2020-2883: ORACLE WEBLOGIC SERVER COHERENCE LIBRARY DESERIALIZATION VULNERABILITY



The [April 2020 Oracle Critical Patch Update \(CPU\)](#) contained patches for several WebLogic flaws, including [CVE-2020-2883](#), a deserialization vulnerability in the Oracle Coherence library of Oracle WebLogic Server. Oracle Coherence is a library used to compress and decompress both serialized and unserialized data. CVE-2020-2883 was disclosed by “[Jang](#),” a researcher quite familiar with Oracle WebLogic vulnerabilities, and Quynh Le of VNPT Information Security Center. This vulnerability was the result of an incomplete patch bypass for [CVE-2020-2555](#), another deserialization vulnerability in the Oracle Coherence library disclosed by Jang and subsequently patched by Oracle as part of the [January 2020 CPU](#). Just two weeks after the release of the April 2020 CPU, Oracle [published a blog post](#) advising the patching of CVE-2020-2883 “without delay” due to active [exploitation in the wild](#). Less than two weeks after Oracle’s blog, a security researcher that goes by the pseudonym of “Y4er” published a [PoC exploit](#) for CVE-2020-2883.

CVE-2020-14625, CVE-2020-14644, CVE-2020-14645 AND CVE-2020-14687: ORACLE WEBLOGIC SERVER CORE COMPONENT VULNERABILITIES



In the [July Oracle CPU release](#), Oracle patched 284 CVEs including [CVE-2020-14625](#), [CVE-2020-14644](#), [CVE-2020-14645](#) and [CVE-2020-14687](#), four vulnerabilities in the Core component of Oracle WebLogic Server. Five days after Oracle’s CPU release, “Y4er” [published a PoC exploit](#) for CVE-2020-14645, further supporting that Y4er is no stranger to Oracle WebLogic Server vulnerabilities.

CVE-2020-14882: ORACLE WEBLOGIC SERVER CONSOLE COMPONENT VULNERABILITIES



As part of the [October 2020 CPU](#), Oracle addressed [CVE-2020-14882](#), an RCE flaw in the Console component of Oracle WebLogic Server. Just one week after the patch was released, Dr. Johannes Ullrich, dean of research at SANS Internet Storm Center, [published a post](#) after observing active scanning and [exploitation in the wild](#) on one of his honeypots. Ulrich noted that these exploits appeared to be based on a [blog post](#) (in Vietnamese) by Jang that contained a detailed analysis which could be used to reproduce a working PoC. Interestingly enough, the attacks Ulrich observed occurred just one day after Jang published his blog. The day after Ulrich’s post, researchers disclosed a bypass for CVE-2020-14882, prompting Oracle to publish an [OOB advisory](#) and a patch for the newly identified flaw identified as [CVE-2020-14750](#). Two weeks after CVE-2020-14882 was patched, a PoC was released, the vulnerability was actively exploited in the wild, a bypass for the patch was reported and a subsequent patch released to address the bypass. Oracle WebLogic Server continues to be a prime target for threat actors and should be high on the list for patch prioritization when Oracle releases its quarterly patches.



CVE-2020-2021: PALO ALTO NETWORKS PAN-OS AUTHENTICATION BYPASS VULNERABILITY



On June 29, Palo Alto Networks [published a security advisory](#) for [CVE-2020-2021](#), a critical authentication bypass vulnerability in the Security Assertion Markup Language (SAML) authentication in PAN-OS devices which received a CVSSv3 score of 10.0. This is a pre-authentication vulnerability, meaning that an attacker does not need local system credentials to exploit the flaw, and if successful, they could access “protected resources” within a network. Based on the description of the vulnerability, organizations running Palo Alto Networks’ GlobalProtect VPN were assumed to be at high risk for exploitation since the application is exposed to the internet, and because the configuration required for the software to be vulnerable is actually quite common across a slew of single sign-on platforms. The vulnerability does not exist in PAN-OS because of these configurations; rather, these configurations allow the exploit to reach the vulnerable code within PAN-OS.



CVE-2019-11510: PULSE CONNECT SECURE ARBITRARY FILE DISCLOSURE VULNERABILITY



Patched in April 2019, [CVE-2019-11510](#) is a pre-authentication arbitrary file disclosure vulnerability in Pulse Connect Secure SSL VPN, formerly known as Juniper SSL VPN. It received a CVSSv3 score of 10.0, highlighting its severity. Just like CVE-2018-13379 in Fortinet’s FortiOS SSL VPN, this vulnerability was discovered and disclosed by Orange Tsai of the DEVCORE research team, who presented their findings in August 2019 at the Black Hat and DEF CON security conferences. Exploitation of CVE-2019-11510 would allow an attacker the ability to access sensitive information, such as the plaintext password that’s stored in a particular file location on the vulnerable device. By itself, CVE-2019-11510 is already a critical vulnerability, but when chained with another vulnerability, it poses an even greater threat. For instance, attackers could combine CVE-2019-11510 with a command injection flaw ([CVE-2019-11539](#)) or a flaw in Pulse Connect Secure’s Network File Share ([CVE-2019-11508](#)) in order to upload a malicious file, leading to full compromise of the system.

CVE-2020-8218: PULSE CONNECT SECURE CODE INJECTION VULNERABILITY

In late August, details about [CVE-2020-8218](#), a code injection vulnerability in Pulse Connect Secure, [was published in a blog post](#) by researchers at GoSecure. The vulnerability was actually [patched on July 27 as part of SA44516](#). It received a CVSSv3 score of 7.2. While the vulnerability is considered post-authentication, it could also be exploited by convincing an admin user to click on a malicious link; attackers have also previously circumvented the valid credentials requirement by leveraging CVE-2019-11510, a pre-authentication arbitrary file disclosure vulnerability in Pulse Connect Secure. Using that vulnerability, attackers have already likely obtained valid credentials for Pulse Connect Secure SSL VPNs. In fact, [a report from ZDNet in August](#) noted that a hacker dumped credentials for over 900 Pulse Secure SSL VPNs.



CVE-2020-6287: SAP NETWEAVER INSUFFICIENT AUTHENTICATION VULNERABILITY



On July 13, SAP [published its monthly SAP Security Patch Day](#). As part of this release, SAP patched [CVE-2020-6287](#), a [critical vulnerability in the LM Configuration Wizard of SAP NetWeaver Application Server JAVA \(AS JAVA\)](#). The vulnerability, which was dubbed “RECON (Remotely Exploitable Code On NetWeaver)” by security researchers at Onapsis, received a CVSSv3 score of 10.0. CISA [published an alert](#) cautioning that the flaw exists by default in SAP applications running on top of SAP NetWeaver AS JAVA version 7.3 and newer. CISA said this vulnerability affects a variety of SAP-related products, including its solutions for Enterprise Resource Planning, Customer Relationship Management, Supply Chain Management and more. SAP NetWeaver is known as the “central foundation” for the SAP software stack because SAP data is accessible over HTTP. The vulnerability stems from a lack of authentication in the LM configuration wizard. An attacker could remotely exploit this vulnerability by accessing the [adm](#) user that has “unlimited access to all local resources related to SAP systems.” They could use this access to create another admin user for their own purposes.

CVE-2020-6286: SAP NETWEAVER AS JAVA INSUFFICIENT INPUT VALIDATION VULNERABILITY

In addition to CVE-2020-6287, SAP also patched CVE-2020-6286, a directory traversal vulnerability in NetWeaver AS JAVA which exists due to an improper input validation for paths under a “certain parameter” of the web service. An attacker could exploit this vulnerability and download a ZIP file from a particular directory. It received a CVSSv3 score of 5.3. PoC exploit code for both CVE-2020-6286 and CVE-2020-6287 are readily available in public repositories on GitHub, which are valuable to cybercriminals looking to simply plug-and-play with these scripts in order to take over devices.

SOPHOS

CVE-2020-12271: SOPHOS XG FIREWALL / SFOS SQLI VULNERABILITY



On April 22, Sophos [published a knowledge base entry](#) on the Sophos Community in response to a zero-day vulnerability discovered in Sophos XG Firewall, which was observed being [exploited in the wild](#). The vulnerability, identified as [CVE-2020-12271](#), is a pre-authentication SQL injection (SQLi) vulnerability that affects the XG Firewall/Sophos Firewall Operating System (SFOS). To exploit the flaw, an attacker would target the XG Firewall’s administration interface via the user portal, which is accessible over HTTPS, or on the wide area network zone. Exploitation of this vulnerability could result in the exfiltration of “XG Firewall-resident data,” including usernames, hashed passwords and local user account credentials, depending on the configuration. This information could then be used in credential stuffing attacks to target other services or applications within an organization. During Sophos’s initial discovery of the vulnerability on a targeted device, researchers observed the presence of malware, which they call Asnarök, that maintains persistence each time the firewall was booted. Sophos [published a separate article](#) providing more details about Asnarök.

TCP/IP LIBRARIES

As operational technology (OT), Internet of Things (IoT) and IT devices continue to find their way into corporate networks, the stakes have never been higher for attackers looking to infiltrate networks. In 2020, there were two significant research efforts surrounding this space: Ripple20 and AMNESIA:33, both of which centered around the discovery of vulnerabilities within the TCP/IP libraries used by millions of OT, IoT and IT devices. Historically, OT devices sought refuge in the safety of air-gapped environments, but they have become more connected over recent years, driven by an evolving IT world and a pursuit of operational efficiency. Many OT environments are complex, sensitive and sometimes dated, with little or no security mechanisms by design and legacy devices that lack security support or have reached end-of-life. Patching or updating to newer devices is sometimes costly or can impact production, resulting in security as an afterthought, superseded by functionality.

Identifying all of the devices affected by these disclosures is a near-impossible task, since the vulnerabilities are found within software libraries that have been used, distributed and re-purposed over decades by dozens of vendors. Adding to the complexity of this supply chain issue, there are also likely vendors who are no longer in business and vulnerable devices that are unsupported, meaning many of these devices may never receive any patches. While vulnerability research on widely used software libraries is not new, these efforts highlight that caution is warranted when vendors decide to use and re-purpose libraries without considering the security implications that may arise.

RIPPLE20: 19 VULNERABILITIES ACROSS OT, IOT AND IT DEVICES



Ripple20 is a set of **19 vulnerabilities** discovered in an embedded TCP/IP software library from Treck Inc., a developer of embedded internet protocols. These 19 vulnerabilities, affecting a variety of OT, IoT and IT devices, range in severity from a maximum CVSSv3 score of 10 down to a low severity score of 3.1. [CVE-2020-11896](#) and [CVE-2020-11897](#), the most severe of the 19 vulnerabilities, can be triggered with malformed packets sent to an affected device and result in RCE or an out-of-bounds write leading to a DoS condition. The vulnerabilities were discovered by researchers at JSOF research lab, and the process to identify affected vendors is ongoing. In collaboration with JSOF, [Tenable Research](#) helped identify potentially affected vendors and devices, and JSOF worked with multiple CERT/CC entities to disclose this information. The following table includes the list of 19 vulnerabilities along with their potential impact and CVSSv3 scores.

CVE	Affected Devices	CVSSv3
CVE-2020-11896	Remote Code Execution	10.0
CVE-2020-11897	Out-of-Bounds Write	10.0
CVE-2020-11901	Remote Code Execution	9.0
CVE-2020-11898	Exposure of Sensitive Information	9.1
CVE-2020-11900	Use After Free	8.2
CVE-2020-11902	Out-of-bounds Read	7.3
CVE-2020-11904	Out-of-Bounds Write	7.3
CVE-2020-11899	Out-of-bounds Read	5.4
CVE-2020-11903	Exposure of Sensitive Information	6.5
CVE-2020-11905	Exposure of Sensitive Information	6.5

CVE	Affected Devices	CVSSv3
CVE-2020-11906	Integer Underflow	6.3
CVE-2020-11907	Integer Underflow	6.3
CVE-2020-11909	Integer Underflow	5.3
CVE-2020-11910	Out-of-bounds Read	5.3
CVE-2020-11911	Incorrect Permission Assignment for Critical Resource	5.3
CVE-2020-11912	Out-of-bounds Read	5.3
CVE-2020-11913	Out-of-bounds Read	5.3
CVE-2020-11914	Out-of-bounds Read	4.3
CVE-2020-11908	Exposure of Sensitive Information	4.3

AMNESIA:33: FOUR OPEN SOURCE TCP/IP LIBRARIES CONTAIN 33 VULNERABILITIES



AMNESIA:33 AMNESIA:33 is a series of 33 vulnerabilities across four open source TCP/IP libraries: uIP, FNET, picoTCP and Ethernut. The bulk of the AMNESIA:33 vulnerabilities center around DoS flaws. However, multiple RCE vulnerabilities were also disclosed, which could allow an attacker to execute code and gain full control over the vulnerable devices. As with Ripple20, the disclosure of these vulnerabilities is an ongoing process, as we expect new vendors to confirm their devices are vulnerable because of the usage of one of these TCP/IP libraries. The following table is a list of the 33 vulnerabilities, the affected libraries, impact and CVSSv3 scores.

CVE	Affected Library	Impact	CVSSv3
CVE-2020-13984	uIP	Denial of Service	7.5
CVE-2020-13985	uIP	Denial of Service	7.5
CVE-2020-13986	uIP	Denial of Service	7.5
CVE-2020-13987	uIP	Denial of Service, Information Leak	8.2
CVE-2020-13988	uIP	Denial of Service	7.5
CVE-2020-17437	uIP	Denial of Service	8.2
CVE-2020-17438	uIP	Denial of Service	7.0
CVE-2020-17439	uIP	DNS Cache Poisoning	8.1
CVE-2020-17440	uIP	Denial of Service	7.5
CVE-2020-24334	uIP	Denial of Service	8.2
CVE-2020-24335	uIP	Denial of Service	7.5
CVE-2020-24336	uIP	Remote Code Execution	9.8
CVE-2020-25112	uIP	Remote Code Execution	8.1
CVE-2020-17441	picoTCP	Denial of Service, Information Leak	7.5
CVE-2020-17442	picoTCP	Denial of Service	7.5
CVE-2020-17443	picoTCP	Denial of Service	8.2

CVE	Affected Library	Impact	CVSSv3
CVE-2020-17444	picoTCP	Denial of Service	7.5
CVE-2020-17445	picoTCP	Denial of Service	7.5
CVE-2020-24337	picoTCP	Denial of Service	7.5
CVE-2020-24338	picoTCP	Remote Code Execution	9.8
CVE-2020-24339	picoTCP	Denial of Service	7.5
CVE-2020-24340	picoTCP	Denial of Service, Information Leak	8.2
CVE-2020-24341	picoTCP	Denial of Service, Information Leak	8.2
CVE-2020-17467	FNET	Information Leak	8.2
CVE-2020-17468	FNET	Denial of Service	7.5
CVE-2020-17469	FNET	Denial of Service	5.9
CVE-2020-17470	FNET	DNS Cache Poisoning	4.0
CVE-2020-24383	FNET	Denial of Service, Information Leak	6.5
CVE-2020-25107	Nut/Net	Denial of Service	7.5
CVE-2020-25108	Nut/Net	Denial of Service	7.5
CVE-2020-25109	Nut/Net	Denial of Service	8.2
CVE-2020-25110	Nut/Net	Denial of Service	8.2
CVE-2020-25111	Nut/Net	Remote Code Execution	9.8



CVE-2020-8467, CVE-2020-8468: APEX ONE/OFFICESCAN VULNERABILITIES



On March 16, Trend Micro [published a security bulletin](#) containing fixes for five vulnerabilities in Apex One and OfficeScan, including [two actively exploited zero-days](#). The first vulnerability, [CVE-2020-8467](#), exists due to a flaw in a component of a migration tool that could result in an authenticated attacker remotely executing arbitrary code on vulnerable installations of these products. The second vulnerability, [CVE-2020-8468](#), is a content validation escape flaw in Apex One and OfficeScan agents that would allow an attacker to “manipulate certain agent client components” if successfully exploited. There were three other vulnerabilities disclosed in the security bulletin, [CVE-2020-8470](#), [CVE-2020-8598](#) and [CVE-2020-8599](#), all of which were assigned CVSSv3 scores of 10 due to their criticality. However, Trend Micro notes no attempts to exploit these three vulnerabilities were observed in the wild at the time the advisory was published.

vBulletin

CVE-2020-17496: VBULLETIN REMOTE CODE EXECUTION VULNERABILITY



Not all zero-day vulnerabilities are discovered after they've been exploited in the wild. A perfect example of this occurred in 2019, when [CVE-2019-16759](#), a critically rated zero-day pre-authentication RCE in popular community forum software vBulletin, [was disclosed anonymously](#) along with a PoC exploit. A patch was released within one day of its anonymous disclosure. Soon after the patch was made available, attackers began exploiting it in the wild, including exploiting the flaw to take down the forums of cybersecurity company Comodo. Nearly a year later on August 9, vulnerability researcher [Amir Etemadieh](#) published a [detailed write-up](#) including a PoC for another zero-day in vBulletin. Identified as [CVE-2020-17496](#), Etemadieh's discovery was the [result of a patch bypass](#) for CVE-2019-16759. According to Etemadieh, the initial patch failed to account for issues present in the template. In a [tweet from Jeff Moss](#), the founder of the DEF CON and Black Hat conferences noted that [DEF CON forums](#) had been targeted "within three hours" of Etemadieh's disclosure. One day later, on August 10, vBulletin [published patches](#) to address the vulnerability for currently supported versions.

vmware®

CVE-2020-4006: VMWARE WORKSPACE ONE COMMAND INJECTION VULNERABILITY



On November 23, VMware [released an advisory](#) for [CVE-2020-4006](#), an authenticated command injection bug in the Identity Manager, Identity Manager Connector, Access and Access Connector components of VMware Workspace One. Exploitation of this vulnerability requires the attacker to be local and authenticated, including a valid password for the configurator administrator account as well as access to the administrative configurator on port 8443. Successful exploitation would result in command execution within the underlying OS without any privilege constraints. Initially, the vulnerability received a CVSSv3 score of 9.1. However, after factoring in the password requirement, the score was lowered to 7.2. The vulnerability was [reported by the NSA](#) as exploited by Russian nation-state actors, marking the agency's second vulnerability disclosure this year, following the CurveBall vulnerability, identified as CVE-2020-0601, in Microsoft's CryptoAPI.



ZOOM: PRIVACY AND SECURITY CONCERNS AT THE VIRTUAL WATERCOOLER

This year, Zoom faced increased scrutiny around its privacy and data collection practices as platform activity increased at breakneck speed, [adding more monthly active users](#) in the first two months of 2020 than in all of 2019. Tenable Research [wrote a blog post](#) about many of these concerns in April, and shortly after, Zoom wrote its own [blog post](#) in response to the numerous privacy concerns that had been raised. Tenable Research has long been interested in Zoom. In 2018, we found and reported [CVE-2018-15715](#), an unauthorized command execution vulnerability that could have allowed an unauthenticated, remote attacker to wreak havoc on Zoom meetings, including the removal of attendees, spoofed messages from users or hijacked screen shares. In early 2020, Alexander Chailytko from Check Point Research [detailed a flaw](#) which he disclosed to Zoom in July 2019. Chailytko found that because Zoom Meeting IDs were 9 to 11 digits long, an attacker could randomly generate IDs and attempt to enter meetings that were not password protected or did not have the waiting room feature enabled. In a phenomenon later known as Zoom-bombing, mischief-makers began capitalizing on the ability to join arbitrary calls to interrupt meetings, share inappropriate content and even threaten participants. As the year progressed, Zoom continued to make improvements to its privacy policies and the security of its services. The company [announced in April](#) that Alex Stamos, former chief security officer at Facebook, was joining Zoom as a consultant, and it planned to “reboot” its bug bounty program. Zoom later announced an acquisition of Keybase to help build out end-to-end encryption, which was rolled out in October. Along the way, the company addressed two path traversal vulnerabilities (CVE-2020-6109, CVE-2020-6110), an encryption flaw (CVE-2020-11500) and a pair of vulnerabilities in the macOS Zoom client (CVE-2020-11469, CVE-2020-11470). Additionally, Zoom addressed a UNC path injection flaw that could have exposed credentials, though this vulnerability did not receive a CVE identifier.

Conclusion

Navigating the rocky terrain of the vulnerability and threat landscape is never easy. The macro challenges of 2020 only added to the difficulties for cyber defenders. As we face the fresh challenges 2021 is sure to bring, here are six lessons to keep in mind:

- **Not every named vulnerability with a logo is critical, nor does every critical vulnerability have a name and a logo.** Ever since the Heartbleed vulnerability was disclosed in 2014, it has become trendy to name vulnerabilities and give them a logo for additional marketability. However, after reviewing the noteworthy vulnerabilities from this year, we found that branding should not be the determining factor when considering the severity of a vulnerability. Look deeper at the CVSS score and other risk metrics, including the availability of proof-of-concept exploits and ease of exploitation. Remember that when it comes to vulnerabilities, context is key.
- **Broken record: Unpatched vulnerabilities are a bigger problem than zero-days.** As long as unpatched vulnerabilities remain a problem for organizations, you can expect us to keep harping on about them. This low-hanging fruit is favored by nation-state actors and run-of-the-mill cybercriminals alike. While zero-day vulnerabilities are often leveraged as part of targeted attacks, unpatched vulnerabilities are targeted en masse, posing a much greater threat. If the software solutions used by your organization are no longer receiving security updates, upgrading to one with an active support contract is vital. It is imperative that organizations identify assets within their environments that are vulnerable to months- and years-old flaws and apply relevant patches immediately.
- **Ransomware remains the biggest threat to organizations today.** According to Chris Krebs, former director of the U.S. Cybersecurity and Infrastructure Security Agency, ransomware is [the most visible, disruptive threat](#) today. The ramifications are not only linked to service disruptions and downtime for employees. When the exposure of proprietary or customer information becomes a bargaining chip leveraged by ransomware groups, the stakes are even higher. Furthermore, the threat of sustained denial of service attacks against an organization's website, their primary communications channel, puts even more pressure on the victims to pay up. It's neither easy nor impossible to thwart ransomware attacks, but it's certainly more beneficial for organizations to go above and beyond, taking all the necessary steps in order to protect themselves.
- **The short and long term impacts of COVID-19 on the workforce.** As the world remains in the throes of COVID-19, many organizations are still adjusting to remote work. For some employees, the lines between their personal lives and places of work have become blurred, with one vulnerability – the human factor – becoming an even more enticing target for threat actors. Much of the infrastructure and implementation that was rapidly stood up to facilitate the work-from-home transition will need to be handled with care and caution in the months ahead. As we've already seen, unpatched vulnerabilities are a prime target for cybercriminals, who are more than ready to take advantage of poor cyber hygiene practices as organizations return to some sense of normalcy. It's important in this climate of uncertainty for organizations to plan ahead and take stock of their assets in anticipation of an eventual shift back to physical offices.
- **Data breaches are mostly attributed to ransomware and email compromises.** Based on our analysis of over 700 breach events, we found that over 35% were caused by ransomware attacks, while 14.4% of breaches were the result of email compromises. Fixing unpatched vulnerabilities, implementing strong security controls for remote desktop protocol, ensuring endpoint security is up-to-date and regularly performing security awareness training are steps organizations can take to thwart some of these attacks. Additionally, 6% of the breach events we analyzed were the result of misconfigured databases and servers, which could provide attackers access to sensitive data without permission. Therefore, it's essential to ensure that proper security controls are in place for your databases and servers, including cloud-hosted services like Amazon Simple Storage Service (S3) and Google Cloud Storage (GCS). Protecting these critical resources can ensure your organization isn't the victim of a data breach due to lax security.

- **Navigating the rugged terrain of vulnerabilities.** As defenders, it's difficult enough to prioritize remediation given the hundreds of vulnerabilities released on Microsoft's Patch Tuesday every month and Oracle's Critical Patch Update each quarter. The 547 vulnerabilities disclosed over the two-month period this summer was unprecedented, and certainly a rollercoaster for any IT administrator. Add in the impact from COVID-19 for defenders trying to protect their newly remote workforce and you have a recipe for chaos. Security teams know to pick their battles, but when there is a flurry of vulnerabilities with a CVSSv3 score of 10.0 released within weeks of each other, the battles are being chosen for you and they're happening simultaneously. In order to manage vulnerability overload, you'll need to take inventory of your entire network, identify your most critical assets and ensure they receive patches in an appropriate time frame. Additional indicators, such as CVSSv3 scores and the availability of PoC exploit scripts, can provide further indicators that a vulnerability is more likely to be exploited in the wild, helping your team focus first on the most severe threats facing your network.



Act now to guard against these vulnerabilities

Considering the depth and breadth of the contents of this report, Tenable will be releasing scan templates for Tenable.io, Tenable.sc and Nessus Professional. These scan templates will cover all of the vulnerabilities discussed throughout this report and will be properly configured to scan your networks for these flaws, enabling you to apply patches in a timely manner and protect your most critical assets. This is the way.

About the Tenable Security Response Team

Tenable Research seeks to step out in front of the curve of the vulnerability management cycle. Our Security Response Team tracks threat and vulnerability intelligence feeds to make sure our plugin teams can deliver coverage to our products as quickly as possible. The SRT also works to dig into technical details and test proof-of-concept attacks when available to ensure customers are fully informed of the risks. The SRT also provides breakdowns for the latest vulnerabilities on the [Tenable blog](#).

Tenable Research has released over 150,000 plugins and leads the industry on CVE coverage. The team is focused on diverse work that makes up the foundations of vulnerability management: writing plugins for vulnerability and asset detection; developing audit and compliance checks; improving VM automation.

About the Authors

[Scott Caveza](#), Research Engineering Manager

[Satnam Narang](#), Staff Research Engineer

[Rody Quinlan](#), Research Engineer

Additional Credits:

[Claire Tills](#), Product Marketing Manager

[Susan Nunziata](#), Senior Director of Editorial & Content

[Matthew King](#), Content Marketing Manager

[Felix Do](#), Graphic Designer



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

01/13/21 V01

COPYRIGHT 2021 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.