



# TENABLE 2022 THREAT LANDSCAPE REPORT

A guide for security professionals to  
navigate the modern attack surface



---

# Contents

<b>Foreword</b> .....	<b>3</b>
<b>Executive Summary</b> .....	<b>5</b>
<b>Methodology</b> .....	<b>9</b>
<b>How to use this report</b> .....	<b>9</b>
<b>Introduction</b> .....	<b>10</b>
<b>SECTION ONE: The Vulnerability Landscape</b> .....	<b>11</b>
<b>Noteworthy vulnerabilities of 2022</b> .....	<b>11</b>
Exchange vulnerabilities favored by a wide array of threat actors .....	11
Disclosure issues complicate defense .....	11
Supply chain vulnerabilities and attacks.....	12
<b>Other vulnerabilities of interest</b> .....	<b>19</b>
<b>The cloud</b> .....	<b>21</b>
Transparency issues.....	21
Data security .....	21
Misconfigurations reign supreme .....	22
Cloud vulnerability discoveries .....	22
<b>SECTION TWO: The Threat Landscape</b> .....	<b>24</b>
<b>Nation state activity</b> .....	<b>24</b>
Known vulnerabilities pose a threat to critical infrastructure and the private sector.....	25
<b>Ransomware: The new normal</b> .....	<b>26</b>
Not all ransomware attacks are made public.....	26
Getting used to the new normal.....	26
The rise and fall of Conti .....	26
Extortion-only attacks rise in prominence .....	27
New ransomware and extortion groups .....	29
Active Directory remains a critical component to successful ransomware attacks .....	30
<b>Breaches</b> .....	<b>31</b>
Unspecified cyberattacks are the root cause of a quarter of breach events.....	33
Why is healthcare the most affected industry? .....	35
Cryptocurrency attacks resulted in the theft of \$2.4 billion dollars.....	36
Understanding trends in cyberattacks through breach data.....	37
<b>Conclusion</b> .....	<b>38</b>
<b>SECTION THREE: A Closer Look at the Key Vulnerabilities of 2022</b> .....	<b>40</b>

# Foreword

## Let's break the cycle

At the start of 2022, cybersecurity teams worldwide were still reeling from the Log4Shell vulnerability, which was disclosed in late 2021. Now, as we head into 2023, the vulnerability – which affected Apache Log4j, a widely used Java logging library – remains a key concern. In fact, when we analyzed a representative sampling of telemetry data we found that, as of October 1, 2022, the vast majority of organizations (72%) remain vulnerable to Log4Shell. Even more concerning, 29% of vulnerable assets saw the reintroduction of Log4Shell after full remediation was achieved.

And Log4Shell was hardly the only risk security organizations had to manage in 2022. The year – marked by macroeconomic shocks spurred by rising inflation and geopolitical upheaval in the wake of Russia's invasion of Ukraine – brought with it the disclosure of even more vulnerabilities in common libraries and dependencies, and an intensification of ransomware attacks.

Perhaps most frustrating of all, we saw known vulnerabilities, in some cases dating back to 2017, still being exploited by attackers. Why? Because organizations have not effectively patched them.

It would be easy for us to point the finger of blame at security organizations for not making vulnerability remediation a priority. It would be easy – and it would also be naive. The reality is that security teams are hampered by a wide array of factors that make vulnerability remediation a challenge. The lesson here is that the broad array of siloed cybersecurity tools and systems organizations have in place is not helping to reduce risk.

We all have to change how we think. As security leaders, our job is to manage risk. Manage exposure.

Manage uncertainty. It starts with taking a holistic view of your attack surface, as offered in this annual Threat Landscape Report, produced by Tenable's Security Response Team (SRT).

In the course of its daily work, Tenable's SRT inspects data from hundreds of sources in order to identify events relevant to our customers and the broader cybersecurity industry. From this vantage point, the team is able to view the vulnerability and threat landscapes holistically to help security professionals identify the trends that matter most. This contextual view is essential for organizations looking to evolve from a reactive cybersecurity posture to one focusing on preventive and proactive measures. We believe

The broad array of siloed cybersecurity tools and systems organizations have in place is not helping to reduce risk.





the modern attack surface – with its mix of on-premises and cloud-based infrastructure, complex identity and access management systems and large numbers of web applications and microservices – demands a more sophisticated approach.

Cybersecurity organizations are well beyond the point where vulnerability management can be performed in a vacuum. It's time to embrace exposure management, a relatively new concept designed to transcend the limitations of siloed security programs. Building an exposure management program involves bringing together data from tools associated with vulnerability management, web application security, cloud security, identity security, attack path analysis and attack surface management and analyzing it in context with your unique mix of users and IT, operational technology (OT) and internet of things (IoT) assets so you can execute a risk-based workflow. Exposure management also provides cybersecurity leaders with the analysis they need to clearly explain the effectiveness of proactive, preventive security programs in a language the business will understand.

Exposure management offers a way to operationalize risk reduction across an organization – and offers a vision of a future in which we no longer see five-year-old vulnerabilities continue to be exploited like a “greatest hits” collection in the attacker playlist.

**Robert Huber**

*CSO and Head of Research,  
Tenable*



---

## Executive Summary

Fresh off the heels of Log4Shell, 2022 began with concerns over supply chains and software bills of material (SBOM) as organizations worldwide were forced to reconceptualize how they respond to incidents in anticipation of the next major event. Tenable's Security Response Team (SRT) continuously monitors the threat landscape throughout the year, putting us at the forefront of trending vulnerabilities and security threats. From this vantage point, we compiled and categorized our data for this annual report.

In a year marked by tense geopolitics, hacktivism, ransomware and attacks targeting critical infrastructure — all alongside a turbulent macroeconomic environment — organizations struggled to keep pace with the demands on their cybersecurity teams and resources. Even as the world faced these challenges, events we observed throughout the year represented a fairly typical year in cybersecurity. Attacks against critical infrastructure remained a common concern. Ransomware continued to wreak havoc, even as some groups had operations shuttered by law enforcement, collapsed under the weight of internal power struggles or splintered into new groups. New vulnerabilities emerged and reliable remediation posed challenges for defenders.

**Perhaps most alarming is that**, alongside the plethora of shiny new vulnerabilities discovered in 2022, the vulnerabilities of years past continue to haunt organizations. In fact, flaws dating back to 2017 were so prominent this year that we felt they warranted the number one spot in our list of top vulnerabilities of 2022.

**We cannot stress this enough:** Threat actors continue to find success with known and proven exploitable vulnerabilities that organizations have failed to patch or remediate successfully.

The constant evolution of the modern digital environment introduces new challenges for security practitioners. Successful security programs must take a comprehensive approach and understand where their most sensitive data and systems lay and what vulnerabilities or misconfigurations pose the greatest risk. Given the brisk rate of digital transformation, a complete understanding of your external attack surface is paramount.

With thousands of new vulnerabilities patched each year, only a small subset will ever see active exploitation.

**By focusing resources on the vulnerabilities** that are exploitable and understanding how attackers chain vulnerabilities and misconfigurations, security teams can design more complete strategies for reducing their overall risk exposure.

This report inspects key aspects of the cybersecurity landscape in 2022 and how organizations can revise their programs accordingly to focus holistically on reducing their exposure. We examine:

**Significant vulnerabilities** disclosed and exploited throughout the year, including how common cloud misconfigurations can affect even tech juggernauts.

**The continuous transformations** of the ransomware ecosystem and the rise of extortion-only threat groups.

**Ongoing risks**, vulnerabilities and attacks within the software supply chain.

**Tactics used by advanced persistent threat groups** to target organizations with cyberespionage as well as disruptive and financially motivated attacks.

**Breach factors and the challenges** in analyzing breach data, given the limited information available and lack of detailed reporting requirements.

**Details of the key vulnerabilities** affecting enterprise software.



# TOP 5 VULNERABILITIES IN 2022

1

Known  
Vulnerabilities  
(2017-2021)

CVE-20XX-XXXX

2

Log4shell:  
Apache Log4j

CVE-2021-44228

3

Follina: Microsoft  
Support Diagnostic  
Tool

CVE-2022-30190

4

Atlassian  
Confluence Server  
and Data Center

CVE-2022-26134

5

ProxyShell:  
Microsoft  
Exchange Server

CVE-2021-34473

# KEY TAKEAWAYS



## Known vulnerabilities play a prominent role in 2022 attacks

In government alerts and industry analysis throughout the year, known vulnerabilities were featured prominently in all types of attacks, including those perpetrated by state-sponsored actors.

Vulnerabilities as old as 2017 are still being successfully exploited in wide-ranging attacks.



## Ransomware attacks intensify, exposing reams of data

2.29 billion records were exposed in 2022. Ransomware continued its domination, accounting for over 35% of data breaches



## Cloud misconfigurations affect even the most mature organizations

Both Microsoft and Amazon experienced breaches of sensitive customer information due to misconfigurations in their own cloud environments. While these incidents did not put customer environments at risk, they demonstrate the importance of minding configurations. Over 3% of all data breaches in 2022 were caused by unsecured databases, accounting for leaks of over 800 million records.



## Supply chain vulnerabilities continue to haunt organizations

Organizations are still contending with the fallout from the Log4Shell vulnerability, disclosed late in 2021, while more vulnerabilities in common libraries and dependencies were disclosed. More than anything, the heightened responses required from IT, security and engineering teams have been extremely disruptive to security operations in 2022.



## Macro factors spur refinements in threat actor behavior

Ransomware remained the largest concern for organizations when reckoning with the threat landscape in 2022, but the groups engaging in these attacks continued to refine their tactics and tools. Geopolitical tensions and nation-state activity also influenced enterprise cybersecurity considerations to a lesser extent.



## Methodology

The 2022 Threat Landscape Report was compiled based on our analysis of the threat landscape throughout 2022. Over the year, SRT tracked government, vendor and researcher advisories, blogs and reports to understand the trends shaping the vulnerability landscape. The breach data for this report was compiled by collecting publicly available information from global news outlets reporting on data breaches from November 2021 through October 2022. The common vulnerability scoring system (CVSS) scores found throughout the report are derived from the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD). In cases where no NVD score is available, scoring is based on the vendor advisory or vulnerability disclosure.

## How to use this report

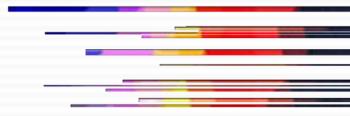
**Reduce your organization's exposure** by identifying and remediating the vulnerabilities and misconfigurations referenced in this report.

**Keep attackers at bay** by learning how threat actors are breaching organizations and the tactics they're employing to hold organizations and their sensitive data for ransom.

**Protect data** by examining some of the common ways data breaches occur and what your organization can do to prevent them.

**Prioritize the vulnerabilities** that are most commonly exploited and maximize the effectiveness of your patching and mitigation strategy.

**Broaden your security controls** to address cloud and identity misconfigurations that attackers continue to target.



# Introduction

Tenable's SRT inspects data from hundreds of sources as part of our day-to-day operations in order to identify events relevant to our customers and the broader cybersecurity industry. As part of our operations, we are able to view the vulnerability and threat landscapes holistically to identify trends. We collect and distill this information each year in our annual Threat Landscape Report (TLR). The insights and guidance we present here aim to help our peers understand how the cybersecurity landscape has evolved so we can all be poised to tackle emerging threats and better secure the world around us.

In [Section One](#), we explore the vulnerability landscape and notable events in 2022 including:

- The ongoing prominence of Microsoft Exchange Server vulnerabilities in attacks
- Log4Shell, notable vulnerabilities and supply chain concerns
- Cloud security issues and misconfigurations

In [Section Two](#), we explore the events that shaped the threat landscape including:

- Nation state activity
- The sustained impact of ransomware and the evolution of the ecosystem and tactics
- Data breach events and key observations drawn from a compilation of publicly available data

In [Section Three](#), we provide a list of all the vulnerabilities discussed in the report, including noteworthy vulnerabilities from these vendors:



## SECTION ONE

# The Vulnerability Landscape

Each year, tens of thousands of vulnerabilities are disclosed by members of the security community and internal research teams at organizations around the world. These vulnerabilities are cataloged by the National Vulnerability Database as Common Vulnerabilities and Exposures (CVEs). Over a five year period from 2018 through 2022, the number of reported CVEs increased at an average annual growth rate of 26.3%. There were 25,112 vulnerabilities reported in 2022 as of January 9, 2023, which represents a 14.4% increase over the 21,957 reported in 2021 and a 287% increase over the 6,447 reported in 2016.

---

## Noteworthy vulnerabilities of 2022

We cannot begin a discussion of noteworthy vulnerabilities in 2022 without mentioning CVE-2021-44228, aka Log4Shell. As soon as it was disclosed at the end of 2021, it was clear the flaw would have considerable effects, but the full depth of its impact took time to emerge. That being said, we've elected to first discuss the longstanding and widespread exploitation of several vulnerabilities in Microsoft Exchange Server due to the years' long exploitation of various attack chains.

### Exchange vulnerabilities favored by a wide array of threat actors

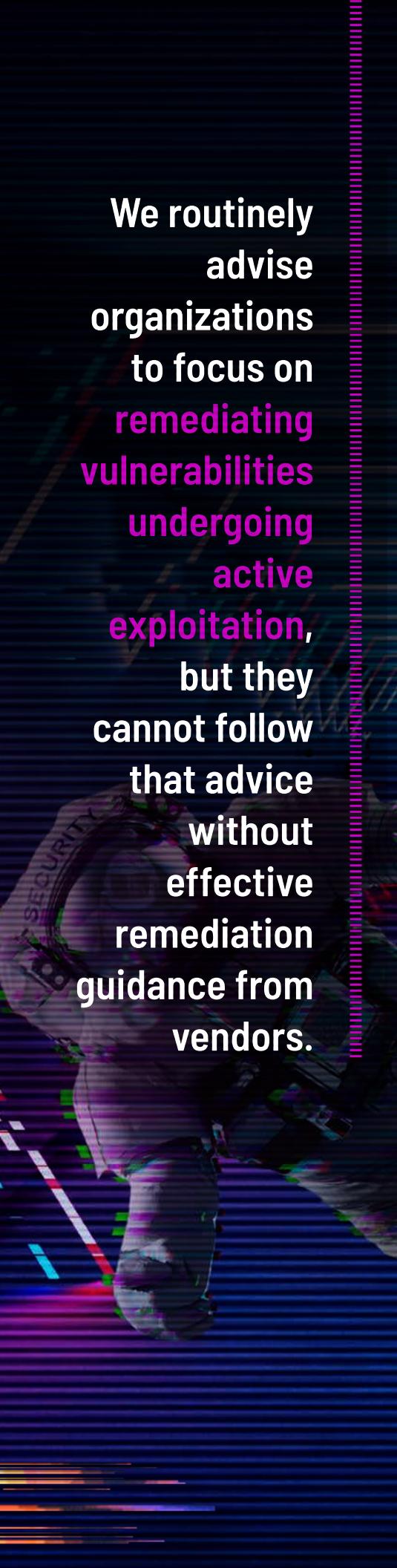
When it comes to breadth of adoption by threat actors, impact on organizations and effects on defenders, vulnerabilities in Microsoft Exchange Server led the pack this year. As noted in our top 5 vulnerabilities for 2022, the ProxyShell chain of vulnerabilities disclosed by Orange Tsai were among the year's highest impact vulnerabilities. Beyond that, threat actors also leveraged ProxyShell's predecessor, ProxyLogon — as well as several vulnerabilities in Microsoft Exchange Server that followed throughout 2022 — to target enterprises around the world.

Attacks targeting vulnerabilities in Microsoft Exchange Server have been attributed to at least 10 unique ransomware groups or strains and half a dozen advanced persistent threat (APT) operations. These vulnerabilities, frequently leading to privilege escalation or remote code execution (RCE), are particularly useful for initial access to target networks.

### Disclosure issues complicate defense

Another troubling theme in the vulnerability landscape this year was a spate of deficient vulnerability disclosures from several major vendors and projects. Many of the most notable incidents involved Microsoft's handling of zero-day vulnerabilities. In May, the research community discovered and confirmed a publicly available exploit for a [remote code execution flaw in the Microsoft Windows Support Diagnostic Tool](#). Initially named Follina due to the lack of CVE assignment, and later designated CVE-2022-30190, Microsoft took more than two weeks to release a patch. Adding to the concern, there were [reports](#) that Microsoft dismissed initial disclosure of the flaw as early as April.

Later in the year, GTSC Cybersecurity Technology Company Limited published information regarding two zero days in [Microsoft Exchange Server \(CVE-2022-41040 and CVE-2022-41082\)](#) that it had seen exploited in the wild. These flaws were dubbed "ProxyNotShell" by the



**We routinely advise organizations to focus on remediating vulnerabilities undergoing active exploitation, but they cannot follow that advice without effective remediation guidance from vendors.**

community. This time, it took Microsoft nearly six weeks to release patches; the company published several iterations of mitigation guidance in the intervening period. These delays to confirm and patch vulnerabilities combined with insufficient guidance make defense even more difficult than it already is. We routinely advise organizations to focus on remediating vulnerabilities undergoing active exploitation, but they cannot follow that advice without effective remediation guidance from vendors.

On the other side of the coin, some vendors created problems through their own proactive behavior. In October, both [Fortinet](#) and [OpenSSL](#) caused confusion by preannouncing vulnerabilities. In both cases, the lack of accurate information available to the public led to rampant speculation and burned resources as security teams were expected to respond and produce results in a vacuum of information. When vulnerabilities can be a critical link in devastating attack chains, and miscommunication puts insurmountable stress on security and engineering teams, vendors must do better to provide quick, but accurate and actionable information.

### Supply chain vulnerabilities and attacks

The [Log4Shell vulnerability](#), disclosed late in 2021, kicked off a second year of supply chain concerns. In the 2021 Threat Landscape Retrospective, we highlighted compromised libraries and repositories and that trend continued through 2022. Python Packaging Index libraries, Node Package Manager (npm), [Javascript](#) packages and [WordPress plugins](#) were all compromised for various purposes – [stealing passwords](#) or [login tokens](#), [installing backdoors](#) and [exfiltrating sensitive data](#).

While 2021 certainly saw significant vulnerabilities in and attacks against supply chains – both software and physical – 2022 was more characterized by the vulnerabilities than the attacks. It felt as if every few months the industry was bracing for “the next Log4Shell.” Rarely did the flaws touted as such match the severity of Log4Shell, but the effects they had on defenders and DevOps teams were nearly as disruptive. Even with the less severe vulnerabilities, organizations had to activate incident response playbooks to cope with demands for information from customers and partners.

Since the 2020 incident targeting organizations via the SolarWinds Orion platform, it feels as if the cybersecurity industry is lurching from one watershed moment to another, with security teams caught in the churn. This issue was apparent with the vulnerabilities in OpenSSL (CVE-2022-3786 and CVE-2022-3602) addressed in early November.

The pre-announcement of the flaw as a critical vulnerability in a key building block of many products and services understandably triggered high intensity responses across security teams. However, the lack of actionable information during the intervening week, and the truth of the lower severity, did not ease the pressure on teams to conjure answers and outcomes. This was the most troubling example, but not the only one, of vulnerabilities that exist on a sliding scale of severity and hype. Vulnerabilities in the Apache Commons Text library (CVE-2022-42889, “Text4Shell”) and the [Spring Framework \(CVE-2022-22965, “Spring4Shell”\)](#) both occupy positions on this scale.

Given the true severity and [long term impact of Log4Shell](#) and the incidents involving SolarWinds and Kaseya, coupled with the inherent uncertainty of vulnerability disclosures, these supply chain vulnerabilities will continue to cause major disruptions, even if they’re never exploited. Until the industry develops better tactics for communicating and operating with uncertainty, precious resources will be expended chasing the wrong vulnerabilities.

# Don't go chasing zero days, patch your known vulnerabilities instead

For 2022, our tracking of zero-day vulnerabilities includes flaws that were exploited in the wild, as well as flaws that were publicly disclosed prior to patches being made available or that do not have patches.

While zero-day vulnerabilities garner a lot of attention, these threats are rarely exploited en masse and instead are used in limited targeted attacks. In many cases, these flaws receive patches quickly and transition into the bucket of vulnerabilities we refer to as known vulnerabilities. Throughout 2022, as part of our analysis of publicly available vendor advisories, disclosures and news articles, we identified 101 zero-day vulnerabilities. For contrast, we identified 105 zero-day vulnerabilities in 2021.

## How quickly zero days transition into known vulnerabilities

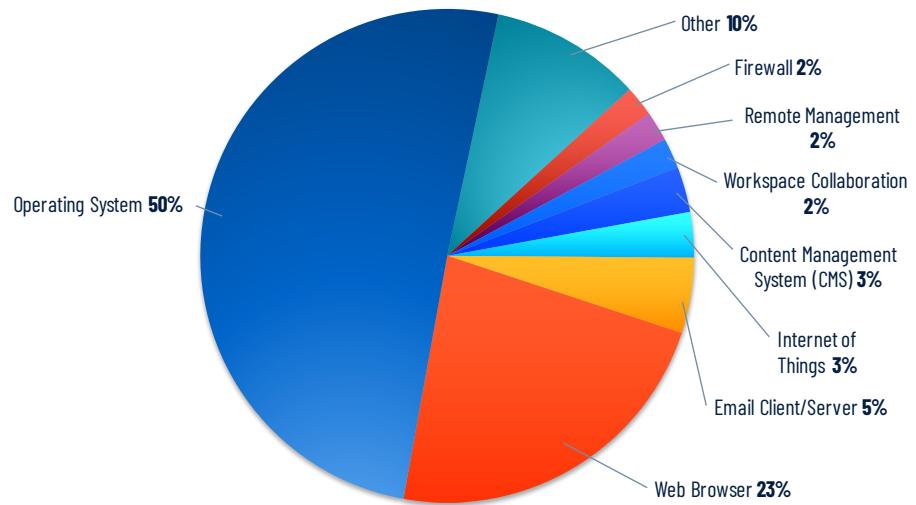
As we evaluate the risk zero days pose, it's important to understand and consider how long they remain unknown to the public — therein lies the danger. Once a zero day is acknowledged by the vendor and a patch is issued, it immediately shifts into the category of known vulnerabilities that security teams can find and fix. When assessing the risk a zero day poses to your organization, it's also important to consider whether it's in, for example, an operating system that's fundamental to all your users, or whether it's a flaw occurring in a specific piece of software used by only a small percentage of your users. This distinction is important to keep in mind as we examine the first five zero-day vulnerabilities of 2022 to be exploited in the wild (see table below). Here, we find that four of these were disclosed to the public on the same day the vendor released patches. While they were used in limited and targeted attacks as zero days, they quickly became known vulnerabilities with actionable guidance from their respective vendors. As we often see, new threats can cause distractions for security teams even if the software in question does not actually pose great risk to the organization because of its limited use. It's imperative to remain vigilant and patch or mitigate the known and exploited vulnerabilities that represent the greatest risk to your organization, instead of focusing on the narrow window in which a zero day exists before a patch is issued.

CVE	Product	Public Disclosure	Patch released
CVE-2022-21882	Microsoft Windows	1/11/2022	1/11/2022
CVE-2021-35247	SolarWinds Serv-U	1/18/2022	1/18/2022
CVE-2022-22587	Apple iOS/iPadOS/macOS	1/26/2022	1/26/2022
CVE-2022-24682	Zimbra Collaboration	12/16/2021	2/5/2022
CVE-2022-22620	Apple iOS/iPadOS/macOS	2/10/2022	2/10/2022

A zero-day vulnerability is a flaw in software or hardware that is unknown to a vendor prior to its public disclosure, or has been publicly disclosed prior to a patch being made available. As soon as a zero day is disclosed and a patch is made available it, of course, joins the pantheon of known vulnerabilities.



### Zero-Days by Software/Hardware Type

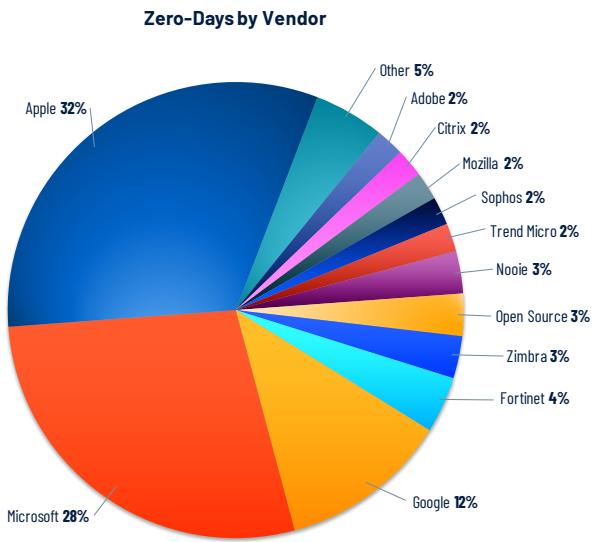


In 2022, we observed stark changes in zero-day vulnerability trends. Unlike the previous two years, where browser-based vulnerabilities led the pack, this year operating system vulnerabilities surged to the top of the charts, accounting for over half of all zero-day vulnerabilities.

### Top Vulnerabilities by Software/Hardware Type

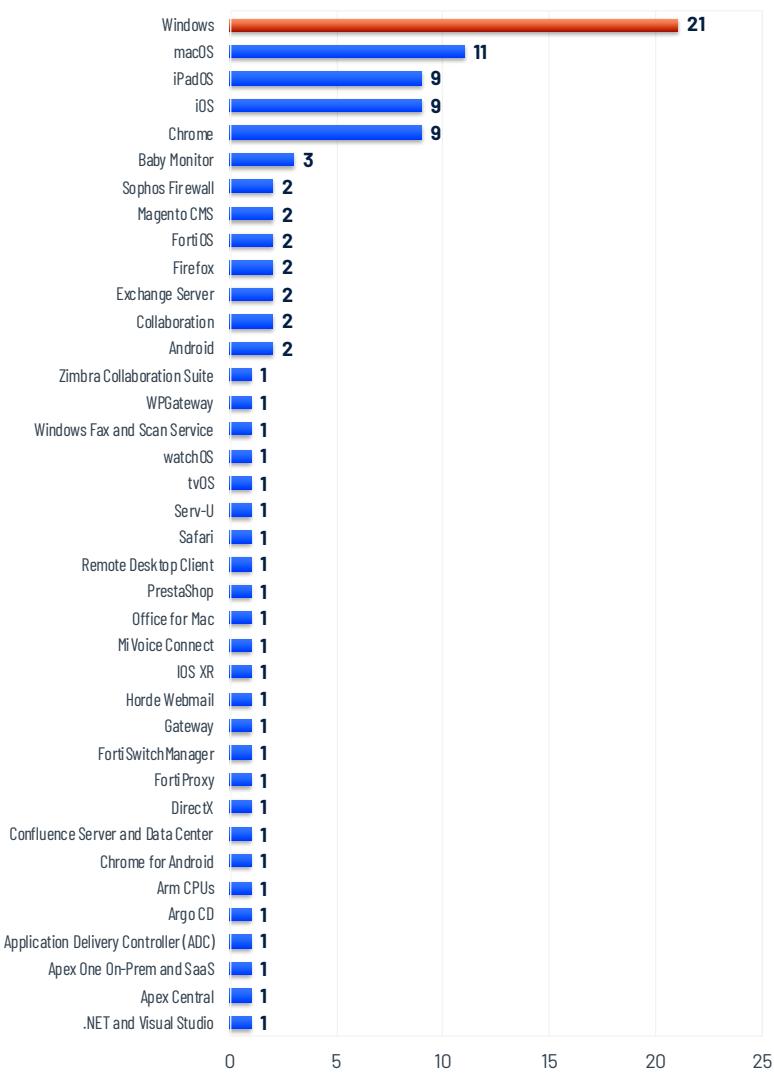
2020	2021	2022
35.7%	30.5%	50.5%
Browser-based vulnerabilities	Browser-based vulnerabilities	Operating system vulnerabilities

The operating system vulnerabilities category includes both native vulnerabilities in operating systems as well as tools and services originating from the operating system itself. These include flaws such as those found in Windows Print Spooler, Windows COM+ Event System Service and more.



As in prior years, the platforms with the largest user base accounted for the greatest number of vulnerabilities in 2022. Zero days in Apple products accounted for 31.7% of all zero-day vulnerabilities, followed by Microsoft at 27.7%. Products from Apple and Microsoft accounted for a combined total of 59.4% of all zero-day vulnerabilities disclosed in 2022.

#### Zero Days by Product



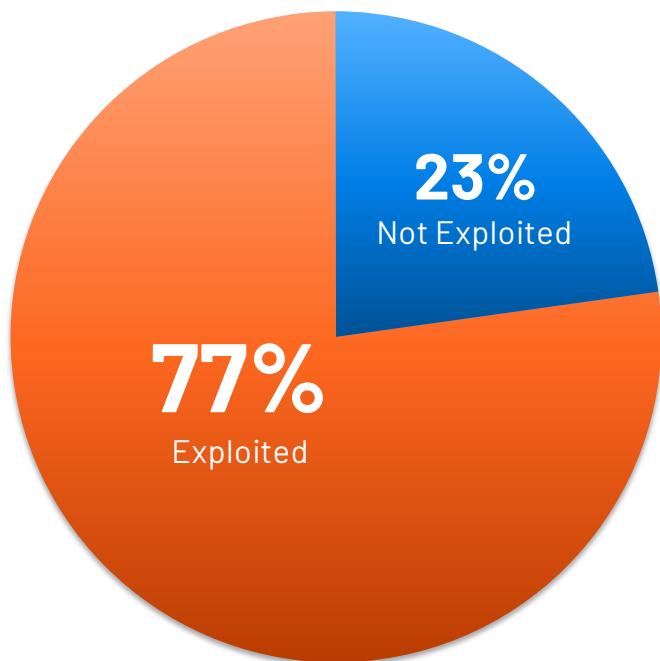
Microsoft Windows vulnerabilities accounted for 21% of all zero days disclosed, followed by a trio of Apple products: macOS (11%); and iOS and iPadOS (9% each). In 2022, Google Chrome vulnerabilities only accounted for 9% of all zero days disclosed.

#### Browser-Based Vulnerabilities Decline

2021	2022
32	23
-	-28.1%

In 2021, 32 browser-based zero days were disclosed and Google's Chrome browser accounted for 17 of them. In 2022, browser-based zero days declined by nearly 30% (28.1%), accounting for 23, nine of which were associated with Google Chrome. It is unclear as to why there was a sharp decline in browser-based zero days, but one theory is that the browser-based sandboxes have made it more difficult for attackers to exploit. Another possibility is that threat actors are pivoting away from zero days and focusing their efforts on known vulnerabilities that remain unpatched.

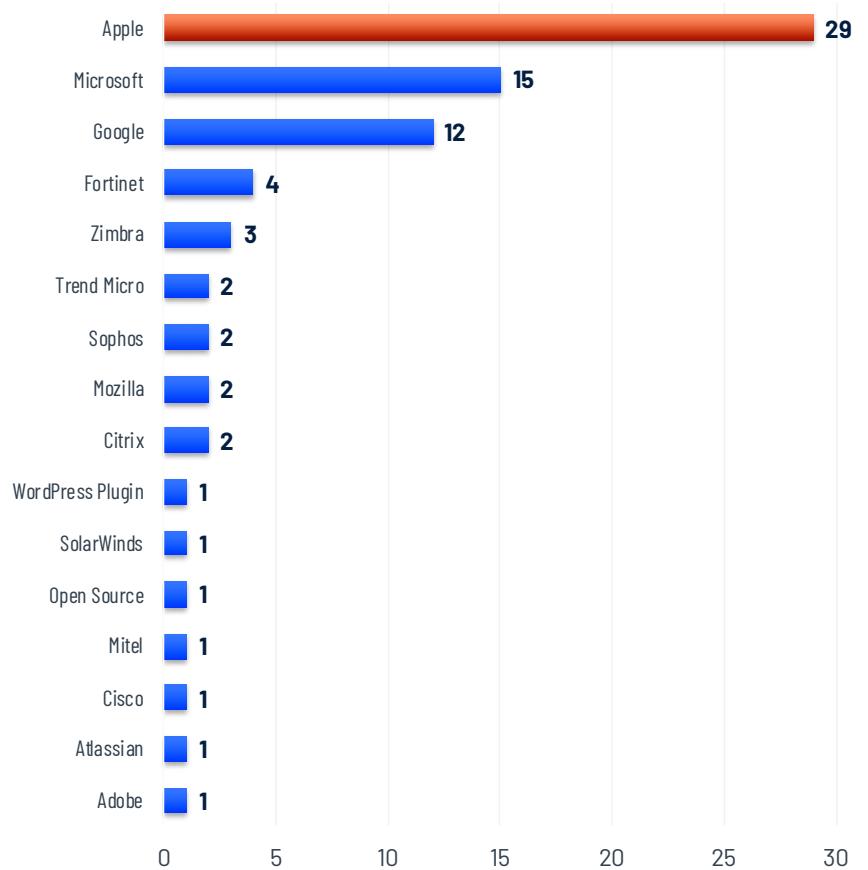
#### Zero Day Vulnerabilities by Exploited Status



The vast majority (77.2%) of zero-day vulnerabilities disclosed in 2022 were exploited in the wild. Yet, this is a 5.8% decrease compared to 2021, which saw 83% of disclosed zero days exploited in the wild.

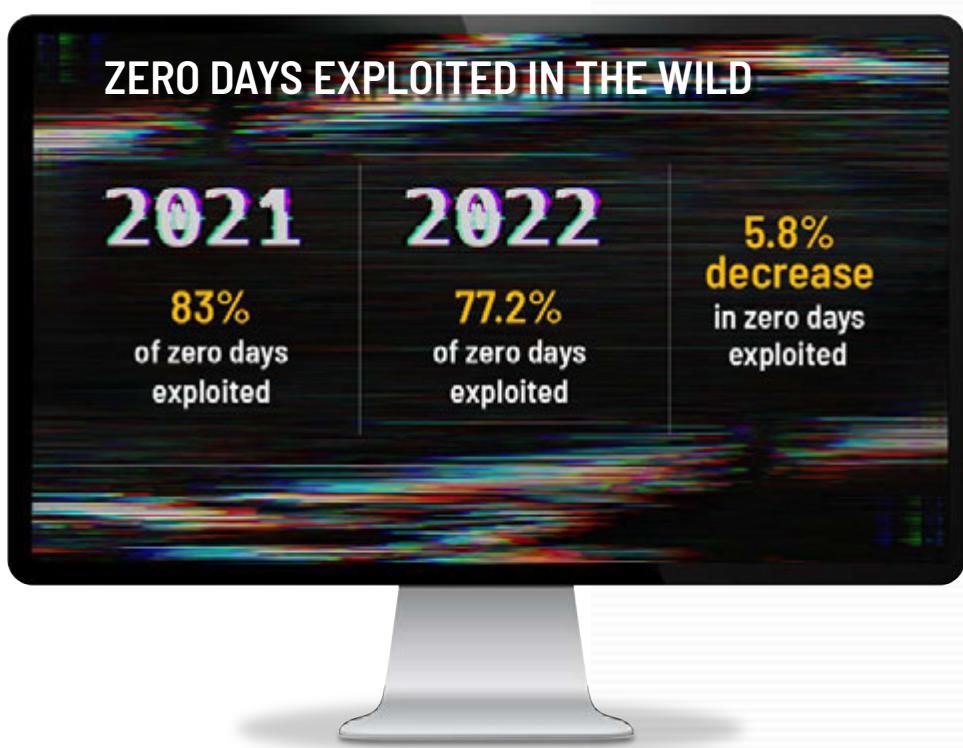
Of the 78 zero days exploited in the wild this year, the lion's share exists in Apple, Microsoft and Google products. Apple accounted for 37.2% of zero days exploited in the wild across multiple products, including iOS, iPadOS and macOS, followed by Microsoft at 19.2%. Google accounted for 15.4%, including Chrome and Android.

## Zero Day Vulnerabilities Exploited in the Wild



Seven vendors had only a single zero-day vulnerability affecting their products.

Four vendors – Citrix, Mozilla, Sophos, and Trend Micro – each accounted for two zero days exploited in the wild, while Zimbra accounted for three. In the case of Fortinet, two zero days affected FortiOS, while one CVE affected both FortiProxy and FortiSwitchManager.





## Do zero days spell trouble for organizations?

Determining the impact a zero-day vulnerability could have on your organization can be challenging. Let's look a little deeper to better understand what a zero day can mean for an organization.

For starters, it's relatively rare for a zero day to be exploited en masse prior to disclosure. Such flaws are most often exploited in limited, targeted attacks. In other cases, zero days are responsibly disclosed by cybersecurity researchers to vendors, who issue patches as quickly as possible.

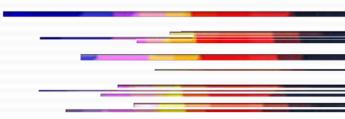
Apple is a case in point. Despite accounting for over a third of zero days exploited in the wild, Apple products, to our knowledge, have not seen widespread exploitation of any zero days in 2022.

On the other hand, CVE-2022-26134, a zero day in Atlassian Confluence Server and Data Center, became one of our top five vulnerabilities in 2022 because we observed a significant increase in exploitation after its disclosure in early June 2022. This vulnerability, which was originally exploited in the wild as a zero day, was first disclosed when Atlassian released the patch to address the issue. In the days that followed this disclosure, exploitation increased as this flaw became a known vulnerability. This flaw poses a significant threat to organizations using affected versions of Confluence Server and Data Center.

It's also important to recognize zero days are often used by attackers to pivot directly into known flaws that are routinely exploited by threat actors of all types including ransomware affiliates and APT groups. ProxyLogon (CVE-2021-26855), a zero day in Microsoft Exchange Server that was disclosed and patched on March 2, 2021, is a prime example of a flaw that started as a zero day and continues to be exploited over a year later by ransomware groups, their affiliates and state-sponsored threat actors.

The bottom line? Vulnerabilities increase risk, whether or not they start as zero days. We advise organizations to operate with a defensive posture by applying available patches for known, exploited vulnerabilities sooner rather than later.

**We advise organizations to operate with a defensive posture by applying available patches for known exploited vulnerabilities sooner rather than later.**



## Other vulnerabilities of interest

While many named vulnerabilities were at the top of our minds throughout 2022 (the various “Shell”s and “Proxy”s), as per usual, unnamed vulnerabilities were as much of a concern. In addition to the unbranded Microsoft Exchange Server vulnerabilities discussed above, there were unnamed flaws in several other widely used products used in attacks.

CVE	Affected product	Description	CVSSv3
CVE-2022-35405	Zoho ManageEngine Password Manager Pro	Unauthenticated RCE	9.8
CVE-2022-26134	Atlassian Confluence Server and Data Center	Object-Graph Navigation Language (OGNL) injection	9.8
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager	Server-side template injection	9.8
CVE-2022-1388	F5 BIG-IP	Authentication bypass	9.8
CVE-2022-40684	Fortinet FortiOS and FortiProxy	Authentication bypass	9.6
CVE-2022-24682	Zimbra Collaboration Suite	Cross-site scripting	6.1
CVE-2022-27924	Zimbra Collaboration Suite	Command injection	7.5
CVE-2022-27925	Zimbra Collaboration Suite	Arbitrary file upload	7.2
CVE-2022-37042	Zimbra Collaboration Suite	Authentication bypass	9.8

Older vulnerabilities also featured prominently among those exploited in attacks. Flaws in Fortinet FortiOS and Zoho ManageEngine were spotted chained in attacks with Log4Shell and various Microsoft Exchange Server vulnerabilities. Attackers continue to target these known vulnerabilities because they continue to be effective, partnering them with newer vulnerabilities and zero days as time goes on. We have been highlighting several of these flaws for years and all of them are listed in the Cybersecurity and Infrastructure Security Agency (CISA) Catalog of Known Exploited Vulnerabilities (KEV).

CVE	Affected product	Description	CVSSv3
CVE-2017-11882	Microsoft Office Equation Editor	Memory corruption	7.8
CVE-2018-0798	Microsoft Office Equation Editor	Memory corruption	8.8
CVE-2018-0802	Microsoft Office Equation Editor	Memory corruption	7.8
CVE-2018-13379	Fortinet FortiOS	Path traversal	9.8
CVE-2020-14882	Oracle WebLogic	Unauthenticated RCE	9.8
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus	Authentication bypass to RCE	9.8
CVE-2021-40444	Microsoft MSHTML (Trident)	Unauthenticated RCE	7.8
CVE-2021-44077	Zoho ManageEngine ServiceDesk Plus	Unauthenticated RCE	9.8

# The cloud

According to a survey conducted by [O'Reilly](#), 90% of respondents are using cloud technologies. As public cloud adoption continues to accelerate, businesses need to adapt to the new complexities in understanding their risk in the world of cloud security. Adopting a cloud-first posture brings new forms of risk, as silent patches and security hardening are often completed by the cloud service providers (CSPs) without any notice. While there is a strong appeal to having a provider like Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure manage aspects of security, the risks posed to the corporate customers of these services are often misunderstood by security and business professionals. As organizations move to these managed cloud services, they lose visibility of their attack surface. They cannot rely on their normal security controls and must trust what is provided by the CSPs.

Security concerns notwithstanding, business drivers such as the need for faster growth and scalability will continue to propel the adoption of public cloud services for organizations of all sizes. As organizations shift their focus to cloud services, care must be taken to ensure security is front of mind – a cloud smart approach. Below we highlight four key areas of concern when it comes to cloud security.

## Transparency issues

One of the biggest challenges organizations face with cloud is that vulnerabilities impacting CSPs are not reported in a security advisory or assigned a CVE identifier; they are often addressed by the CSP without notice to the end user. This lack of transparency makes risk assessment challenging. Without release notes, security advisories or any identifier for tracking, infosec teams face massive challenges in evaluating the security posture of a cloud provider. Adding to the difficulty, many providers fail to mention when incident response processes are kicked off or whether any evidence of exploitation of a reported vulnerability has occurred. The many blind spots these practices create for organizations are a growing concern. While there is much debate on how to track these vulnerabilities, no solution exists today.

## Data security

While each CSP offers its own [best practices](#), with tips on proper access controls, we continue to observe data breaches caused by unsecured or improperly secured cloud resources. This year, [Microsoft disclosed](#) that it had a misconfigured and unsecured Azure endpoint that potentially allowed access to business transaction data of Microsoft and prospective customers. The issue was reported to Microsoft by [SOCRadar](#) and highlights that even CSPs are subject to misconfiguration mistakes.

**Cloud Service Providers (CSP)** are companies that provide the infrastructure and components used for cloud computing, including private and public cloud resources. Private clouds are environments dedicated to a single entity and can be easily isolated to groups and users as necessary. Public clouds are developed to allocate resources to multiple tenants and clients, typically managed by third-party providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.



In another example, Amazon faced a data security incident when a researcher found an [unsecured Elasticsearch database](#) containing Amazon Prime user viewing data. With over 215 million entries in the database, even pseudonymized data being leaked is concerning for any end user of the service.

The above examples illustrate how even massive CSPs owned by giant tech titans are not immune from simple configuration mistakes. From our own analysis of publicly reported data breaches, we found that over 3% of data breaches disclosed in 2022 resulted from an unsecured database. These data breaches, collectively, exposed over 800 million records across a variety of industry verticals.

## Misconfigurations reign supreme

Going beyond unsecured and open databases, a variety of cloud configuration mistakes can open the door to risk for organizations. Kubernetes, one of the de-facto container management platforms, is a particular area of concern. A study from the [Cloud Native Computing Foundation](#) conducted in 2021 found that 96% of respondents were using Kubernetes and nearly 70% were using Kubernetes in production. In a recent study, conducted by researchers at the [Shadowserver Foundation](#), 84% of identifiable Kubernetes API instances were exposed to the internet. As the report indicates, this does not suggest that each of these is vulnerable, but it's unlikely that there are valid reasons to have these APIs exposed. In 2021, researchers at [Trend Micro](#) detailed how a malicious group known as TeamTNT compromised thousands of Kubernetes clusters to install cryptomining applications by abusing the Kublet API, which had been left exposed on each of the targeted clusters.

With Kubernetes being such an attractive target for threat actors, the U.S. National Security Agency (NSA) and CISA continue to provide updates to their [joint technical report](#) on Kubernetes Hardening to help encourage secure practices and best practices for Kubernetes deployments.

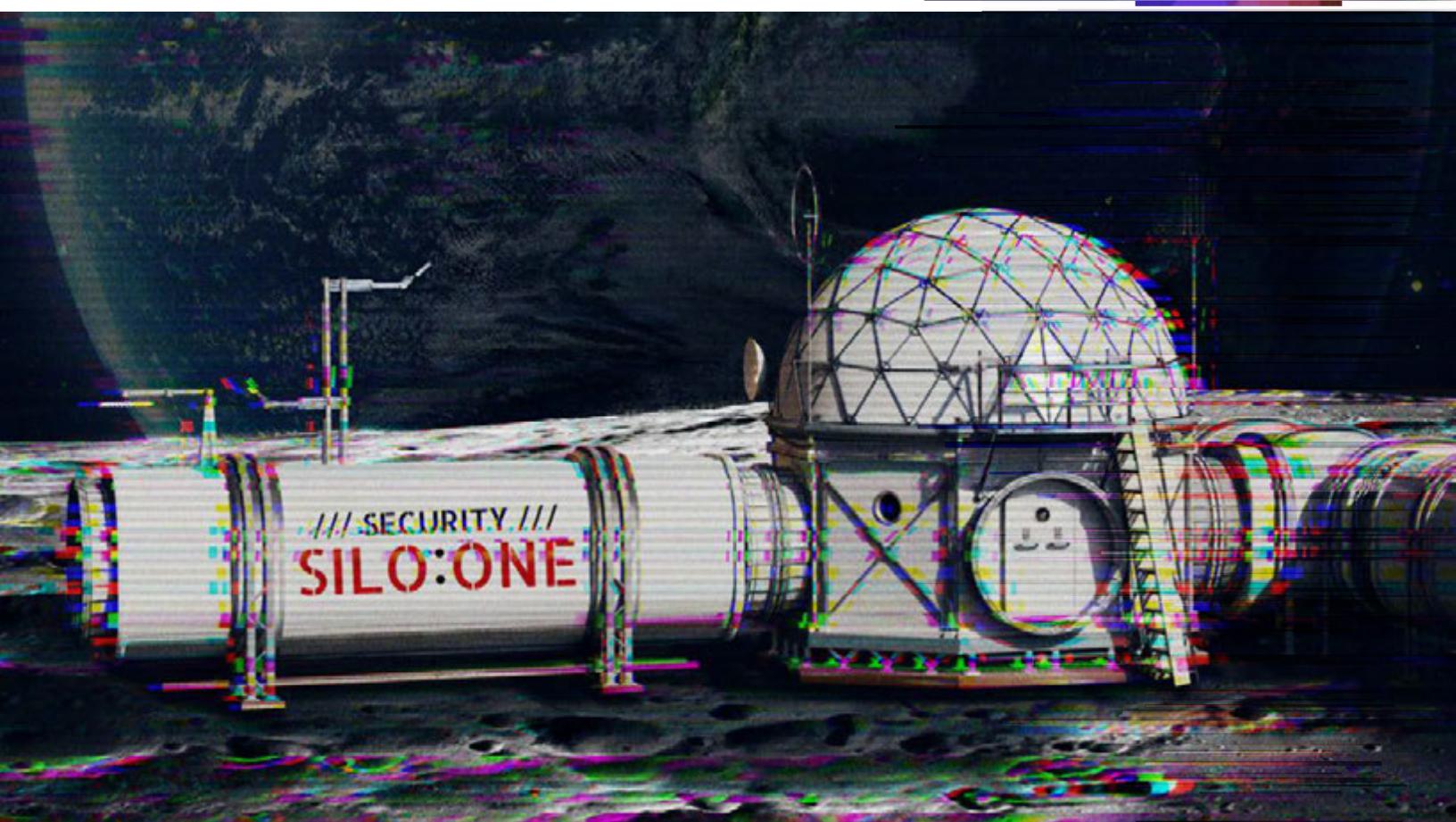
## Cloud vulnerability discoveries

Throughout the year, multiple discoveries were made and reported to CSPs from a variety of independent researchers and companies. As noted above, in many instances the only information about cloud vulnerability discoveries came from write-ups released by security researchers, rather than the CSPs. With dozens of services from CSPs in use by enterprises worldwide, researchers are only just scratching the surface of these mammoth targets.

Tenable researcher Jimi Sebree made several discoveries from his work on Microsoft Azure as outlined in the following table:

Product	CVE	Vulnerability Type	CVSSv3 Score
Microsoft Azure Synapse Analytics	N/A	Privilege Escalation	N/A - Critical severity
Microsoft Azure Synapse Analytics	N/A	Hosts File Poisoning	N/A - Low severity
Microsoft Azure Site Recovery	CVE-2022-33675	Privilege Escalation	7.8
Microsoft Azure Arc	N/A	Information Disclosure	6.5

With a lack of transparency around cloud vulnerabilities, users of these services are unlikely to have a true understanding of the risk presented to their cloud resources. While some vulnerabilities will get CVEs or security advisories, others may be silently fixed by a CSP. These factors make evaluating the security posture of one provider over another a daunting task for security professionals. As they continue to embrace the public cloud, organizations need to plan ahead to ensure they are evaluating their own practices and that of their CSPs to keep the focus on secure cloud deployments. It's safe to assume that cloud services would have a similar occurrence of vulnerabilities to their on-premises counterparts, but the lack of transparency leaves cloud users in the dark about their risk exposure.



## SECTION TWO

# The Threat Landscape

Analyzing the vulnerability landscape alone only tells part of the story. We also need to understand the threat landscape: how attackers are using those vulnerabilities, along with other tools and tactics, to target enterprises, governments and nonprofits. Let's explore the key features of the threat landscape in 2022 and how defenders should meet these latest challenges.

## Nation state activity

Cyberattacks conducted by or at the behest of nation states are a constant concern in the threat landscape. This was particularly true in 2022 as geopolitical tensions, elections and world events influenced enterprise cybersecurity considerations.

At the start of 2022, multiple U.S. government agencies including CISA, the Federal Bureau of Investigation (FBI) and NSA [issued a joint cybersecurity advisory \(AA22-011A\)](#) providing a list of tactics, techniques and procedures (TTPs) used as part of cyber operations conducted by Russian state-sponsored threat actors. The advisory included a list of known vulnerabilities used by Russian state-sponsored APT groups. A separate advisory from the same U.S. agencies in February 2022 confirmed that Russian state-sponsored cyber actors have regularly targeted U.S.-cleared defense contractors. This advisory was published shortly before Russia began its invasion of Ukraine on February 24, 2022.

In March, as part of a [press briefing regarding cyberthreats to the United States](#), deputy national security advisor for the Biden administration, Anne Neuberger, issued a call to action to the private sector regarding potential cyberattacks conducted by the Russian state against critical infrastructure. In her briefing, Neuberger highlighted what she called the “most troubling piece” being the presence of “known vulnerabilities” being used by “even sophisticated cyber actors to compromise American companies, to compromise companies around the world” making it “far easier for attackers than it needs to be.”

**“The most troubling piece and really one I mentioned a moment ago is we continue to see known vulnerabilities, for which we have patches available, used by even sophisticated cyber actors to compromise American companies, to compromise companies around the world. And [...] that makes it far easier for attackers than it needs to be.”**

– Anne Neuberger, Deputy national security advisor for the Biden administration

In November 2021, CISA released [Binding Operational Directive 22-01](#), which mandates remediation timelines for known exploited vulnerabilities in Federal Civilian Executive Branch agencies and organizations. Alongside the directive, CISA established its KEV catalog to track significant vulnerabilities that have been observed used in attacks. Since its release, the KEV has become a useful prioritization tool for organizations in all sectors.

In September, U.S. agencies – along with the Australian Cybersecurity Centre, the Canadian Centre for Cyber Security and the U.K.’s National Cyber Security Centre – [published a joint cybersecurity advisory \(AA22-257A\)](#) regarding APT activity affiliated with Iran’s Islamic Revolutionary Guard Corps (IRGC). This is a follow-up to a previous [advisory issued by these agencies in November 2021 \(AA21-321A\)](#). Unsurprisingly, the latest advisory highlights some of the known vulnerabilities exploited by IRGC-affiliated APT actors, including Log4Shell, ProxyShell and flaws in Fortinet’s FortiOS (discussed earlier in the Noteworthy section of this report).

In June, CISA, the NSA and the FBI issued a joint cybersecurity advisory detailing the use of publicly known vulnerabilities by state-sponsored actors affiliated with the People’s Republic of China (PRC). This was followed by a [separate joint cybersecurity advisory \(AA22-279A\)](#) from the same agencies in October, detailing the Top 20 CVEs that have been actively exploited by PRC state-sponsored cyber actors.

## Known vulnerabilities pose a threat to critical infrastructure and the private sector

One key theme across these government advisories is that known vulnerabilities with available patches are being routinely exploited to gain initial access into organizations and to elevate privileges once inside. In fact, when we look at all the advisories collectively, there are a number of overlapping vulnerabilities being used by each of these state-sponsored threat actors.

Overlapping CVEs	Product type	State-sponsored exploitation
CVE-2018-13379	SSL VPN	Iran, Russia
CVE-2019-11510	SSL VPN	PRC, Russia
CVE-2019-19781	SSL VPN	PRC, Russia
CVE-2020-0688	Email Server	Iran, Russia
CVE-2020-5902	Traffic Management Server	PRC, Russia
CVE-2021-26855	Email Server	PRC, Russia
CVE-2021-26857	Email Server	PRC, Russia
CVE-2021-26858	Email Server	PRC, Russia
CVE-2021-27065	Email Server	PRC, Russia
CVE-2021-44228	Logging Library	PRC, Iran

We’ve covered many of the overlapping flaws in prior Threat Landscape reports, including the trio of SSL VPN flaws and email server vulnerabilities like ProxyLogon. These types of widely used products are routinely exploited each year by a variety of threat actors, including these state-sponsored threat actors. There’s a clear way to stop these flaws from remaining staples in attacker toolkits: Apply the available patches. We’d like to see these known vulnerabilities disappear from future versions of this report.

**"We've only seen the problem continue to get worse [...] We've seen a higher volume of ransomware attacks and the financial losses are increasing as well."**

— Paul Abbate,  
deputy director, FBI

## Ransomware: The new normal

*For an overview of the various players involved in ransomware attacks, please refer to our [Ransomware Ecosystem report](#) released in June 2022.*

Throughout 2022, there have been [reports that ransomware attacks have seen a decline](#) compared to previous years. However, the data we analyzed for this year's Threat Landscape Report shows the frequency of ransomware attacks remaining on par with prior years. According to our analysis of publicly available breach data, 35.5% of breaches in 2022 were the result of a ransomware attack, a 2.5% decrease from 2021.

At the Aspen Cyber Summit in November, Paul Abbate, deputy director at the FBI [said that](#) the agency has "only seen the problem continue to get worse" and has "seen a higher volume of ransomware attacks and the financial losses are increasing as well."

### Not all ransomware attacks are made public

One of the ways we quantify ransomware attacks in our analysis is through news reports, and the other is through entries on ransomware leak websites. On these websites, ransomware groups threaten to publish stolen data from victim organizations. The one challenge with relying on leak website data is that there may be instances where an organization chooses to pay the ransom demand before the group can post an entry on its leak website, making metrics drawn from these sites somewhat unreliable.

Another challenge is that not all ransomware attacks are known to the public. In some cases, businesses use careful generic language, such as "cyberattack" or "incident," when announcing a data breach or security event. Countries and affected sectors have different reporting requirements, and there is no universal requirement for organizations to report the root cause of an incident, though some may choose to disclose that information. This makes it challenging to truly quantify not just ransomware attacks, but breaches in general. So it's important to recognize that the true number of ransomware attacks over the last few years has likely been significantly undercounted.

### Getting used to the new normal

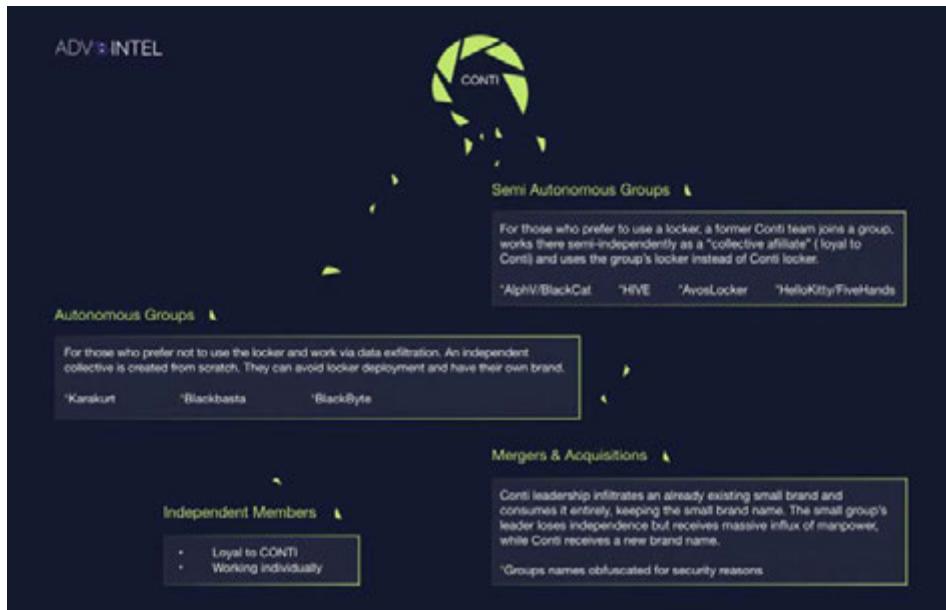
In the winter months, when it's cloudy all the time, the novelty of it being cloudy wears off quickly. In the threat landscape, the novelty of ransomware attacks has worn off, yet they still remain prominent. Ransomware attacks have become the new normal.

### The rise and fall of Conti

Conti, a ransomware group that rose to notoriety over a two-year period during which it earned at least \$180 million in profits, shuttered its operations in May 2022. The fall of Conti was considered a win by many, as it had cemented itself as one of the most dominant

ransomware groups over the last few years. However, as we've seen in the past with the disappearance of other ransomware groups like DarkSide and BlackMatter, this isn't the end of the road for Conti, its members or the group's tactics and techniques.

According to researchers at Advanced Intel, who were the [first to report on Conti's exit from the ransomware ecosystem](#), Conti's existing partnerships with other ransomware groups, including ALPHV/BlackCat, Hive, AvosLocker and HelloKitty/FiveHands, allowed its members to join those groups, where they offered assistance with development, pentesting, intelligence and negotiations.



*Image Source: Advanced Intel*

Independent members, whom Advanced Intel says are "loyal to Conti," will likely operate individually, possibly as affiliates for other groups. Finally, some former members of Conti have transitioned to groups that focus purely on data exfiltration for extortion-only operations, which includes groups like Karakurt, Black Basta and Blackbyte.

In the ransomware ecosystem, groups are not the constant; it's the group members, including affiliates, that remain a prominent fixture, which is why the long term impact of a ransomware group's demise is blunted.

## Extortion-only attacks rise in prominence

Ransomware attacks have enjoyed immense success through double extortion techniques, which involve:

1. encrypting files on a targeted network; and
2. the exfiltration and threat to publish stolen data

A key feature in the threat landscape of 2022 was the increased prevalence of extortion-only attacks. In such attacks, threat actors access target networks with the specific purpose of exfiltrating sensitive data to hold for ransom or sell on the dark web, without deploying any of the encryption malware that gives ransomware its name. Groups taking an extortion-only



approach were on a tear throughout 2022. Most notable was the LAPSUS\$ group, which exfiltrated data from several companies in South America and Europe, as well as prominent technology companies like Microsoft, Okta and Nvidia. Some Conti group members also joined existing extortion-only operations like Karakurt.

These groups often deployed more “simplistic” tactics, relying on phishing, spamming multifactor authentication (MFA) and exploiting help desk services to gain access to target environments. As with their ransomware counterparts, extortion-only groups seek access to high privileged accounts through Active Directory (AD), abusing flaws, misconfigurations and features of the ubiquitous Microsoft identity and access management tool. They also target cloud resources to support attack infrastructure and to access sensitive data.

Organizations cannot afford to ignore these threat actors because they appear “less sophisticated.” Their attacks can be just as disruptive as ransomware and represent considerable risk to ongoing operations and organizational reputation. Additionally, the more sophisticated ransomware groups have even adopted extortion-only habits as an evolution of their playbooks.

The following guidance will help organizations defend against attacks from extortion groups:

- Reevaluate help desk policies and social engineering awareness
- Strengthen password policies: avoid SMS-based MFA; ensure strong password use; leverage passwordless authentication
- Use robust authentication options for internet-facing applications
- Find and patch known exploited vulnerabilities that could allow attackers to elevate privileges and exfiltrate sensitive data
- Bolster cloud security posture: improve risk detections, strengthen access configurations
- Ensure identity security services like AD are appropriately configured according to zero trust best practices

## New ransomware and extortion groups

From November 1, 2021 to October 31, 2022, at least 31 new ransomware and extortion groups were discovered.

Group	Type	Discovery date
ALPHV/BlackCat	Ransomware	November 2021
Rook	Ransomware	November 2021
Sugar	Ransomware	November 2021
Night Sky	Ransomware	December 2021
White Rabbit	Ransomware	December 2021
RansomHouse	Extortion	December 2021
Ransom Cartel	Ransomware	December 2021
Royal	Ransomware	January 2022
Entropy	Ransomware	February 2022
Pandora	Ransomware	March 2022
Luna Moth	Extortion	March 2022
Black Basta	Ransomware	April 2022
DarkAngels	Ransomware	May 2022
Cheerscrypt	Ransomware	May 2022
Omega	Ransomware	May 2022
Checkmate	Ransomware	May 2022
BlueSky/Blue Sky	Ransomware	May 2022
Luna	Ransomware	June 2022
GwisiLocker	Ransomware	June 2022
Play	Ransomware	June 2022
RedAlert(N13V)	Ransomware	July 2022
HavanaCrypt	Ransomware	July 2022
Lilith	Ransomware	July 2022
BianLian	Ransomware	July 2022
Monti	Ransomware	July 2022
Donut Leaks	Extortion	August 2022
Agenda	Ransomware	August 2022
Venus	Ransomware	August 2022
TommyLeaks/SchoolBoys	Extortion	September 2022
Hardbit	Ransomware	October 2022
Prestige	Ransomware	October 2022

This information is based on publicly available sources including news outlets and vendor blog posts and may not reflect all the new ransomware or extortion groups.



With the fall of Conti, other ransomware groups have risen to pick up the pieces. ALPHV/BlackCat is one such group. It has emerged as one of the top ransomware groups in operation today in terms of its execution and volume of ransomware attacks.

## Active Directory remains a critical component to successful ransomware attacks

Compromise of Active Directory remains a key element in enabling ransomware to achieve its goals of domain-wide systems encryption and data exfiltration to facilitate double extortion. Like the Marvel villain Thanos, AD compromise is inevitable. In 2022, researchers at the DFIR Report [highlighted one of the fastest ransomware cases](#), involving the Quantum ransomware, which resulted in the propagation of domain-wide ransomware in under four hours. In this instance, it was the use of [AdFind](#), a tool for collecting information on AD, that ultimately resulted in the domain wide ransomware deployment. Ransomware groups have also historically leveraged a variety of vulnerabilities to elevate privileges to domain administrator inside a victim organization, including CVE-2020-1472, an Elevation of Privilege (EoP) vulnerability in Windows Netlogon also known as Zerologon, and CVE-2021-36942, a spoofing vulnerability in the Windows Local Security Authority, also known as PetitPotam that Microsoft calls a “classic NTLM Relay Attack.” Despite the availability of patches for PetitPotam, Windows New Technology LAN Manager (NTLM) relay attacks are still possible, so organizations need to apply additional mitigations which are outlined [here](#).

The exploitation of these flaws, combined with a variety of tools leveraged by ransomware groups to collect vital AD information, highlight the importance of identifying [indicators of exposure](#) and [indicators of attack](#) within your AD environments. By [hardening AD against ransomware attacks](#), organizations can hinder these groups’ attempts to encrypt and exfiltrate stolen data for leverage and allow your organization to operate from a position of defense.



## Breaches

Tenable's breach statistics were captured from November 1, 2021 through October 31, 2022 and include breaches dated within the specified period as well as breaches reported in that timeframe that lacked a breach date.

As part of our monitoring of the threat landscape, Tenable's SRT tracks breach reports on a daily basis in order to track trends at a macro level. In 2022, we tracked 1,335 breach events during the specified period above, a 26.8% decrease from the 1,825 we tracked during the same period a year earlier.

Our analysis of these breach incidents is performed on a best-effort basis and is not intended to be a fully exhaustive list of all the breaches reported throughout this time period. Based on our past examination of breach data, we recognize that the disclosure process for breaches takes time and, therefore, some breaches may not be made public until months or years after the incident occurs. Additionally, we must also acknowledge that some industries and geographic locations have varying or sometimes even no reporting requirements or central authority for reporting. This makes obtaining a comprehensive global view of the breaches that occurred over this time period nearly impossible.

In 2022, the breach events we analyzed resulted in the exposure of 2.29 billion records, a marked decrease compared to 2021, where 40 billion records were exposed. This was matched by a comparable decline in the number of files exposed in 2022 – 389 million – a figure which includes both documents and emails. Despite the steep decline in records and files exposed, the total volume of data exposed as part of breach events in 2022 remained flat at 257 Terabytes, compared with 260 Terabytes in 2021.

Of the 1,335 breach events tracked in 2022, 88.2% of the impacted organizations reported that records were exposed. However, 45% did not disclose a number of records exposed, while for 6.1% of breaches the impacted organizations could not confirm whether or not records were exposed.

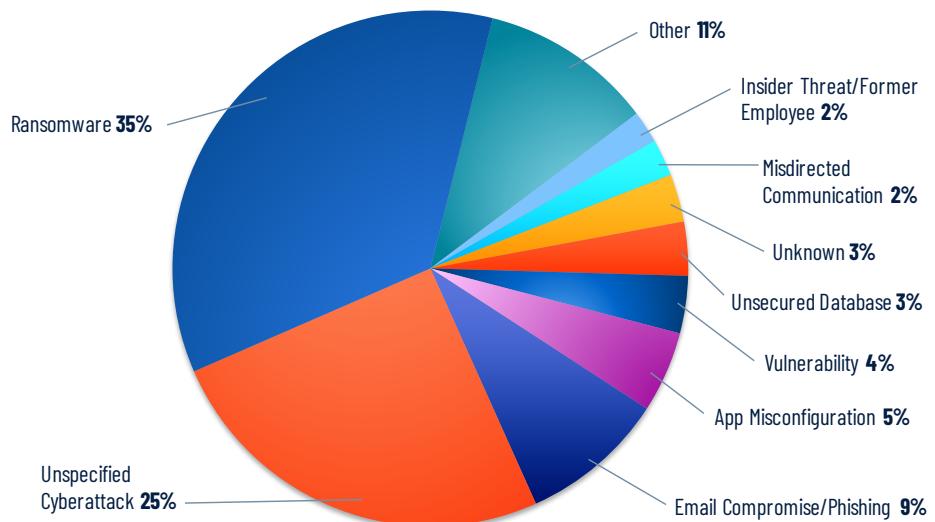
Over 2.2 billion records were exposed in 2022

DATA POINT	2021	2022
<b>Total records exposed</b>	<b>40,000,000,000</b>	<b>2,296,941,687</b>
<b>Total files exposed</b>	<b>1,800,000,000</b>	<b>389,127,450</b>
<b>Total data exposed</b>	<b>260 Terabytes</b>	<b>257 Terabytes</b>

Region	Total records exposed	% of total
Asia-Pacific (APAC)	1,561,990,339	68.00%
North America (NAM)	405,954,391	17.67%
Europe, Middle East, and Africa (EMEA)	305,994,856	13.32%
Unknown/Global	22,540,901	0.98%
Latin America (LATAM)	461,200	0.02%
<b>Totals</b>	<b>2,296,941,687</b>	

More than two thirds (68%) of records exposed originated from organizations located in Asia-Pacific (APAC). Organizations in North America (NAM) and Europe, Middle East, and Africa (EMEA) accounted for a combined 31% of records exposed. In some instances, it was unclear what region an organization was located in, so we categorized such breach events as Unknown/Global. Finally, breach events in Latin America (LATAM) accounted for just 0.02% of records exposed. We speculate this stark difference has more to do with the different breach reporting requirements in LATAM countries, compared to NAM, APAC and EMEA, than an appreciable difference in attacker activities in the various regions.

### 2022 Breaches by Root Cause

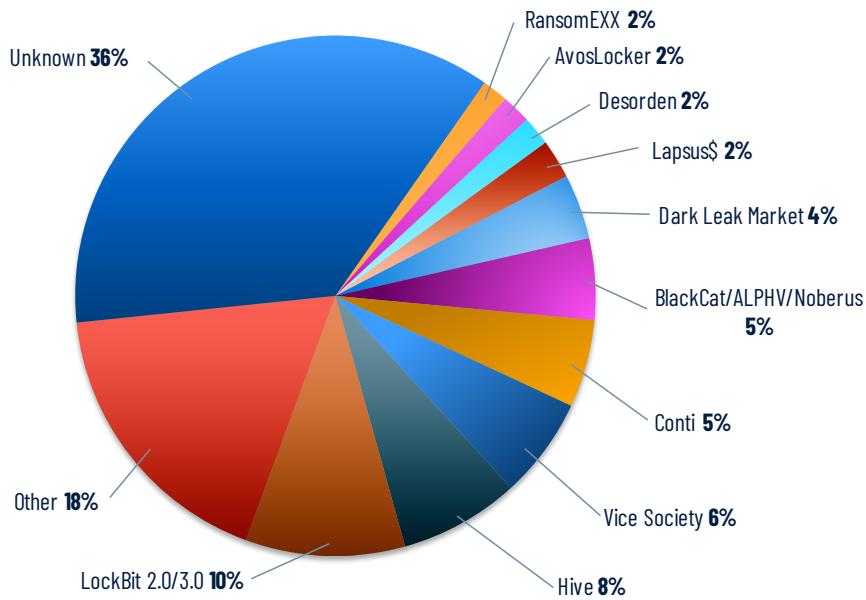


In 2022, ransomware remained the most common root cause for breaches at organizations, accounting for 35.4% of all breach events. This is a slight decrease compared to 2021, in which ransomware represented 38% of all breach events.

### Ransomware Events as a Percentage of All Breach Events

2022	2021	2020
35.4%	38%	35%

## 2022 Ransomware/Extortion Attacks



When reviewing all of the breach events linked to ransomware or extortion attacks, we classified nearly half (36.4%) as “Unknown,” as we could not identify any specific details about the ransomware or extortion group responsible for these attacks. We also attempted to cross-reference these attacks against data leak sites on the dark web associated with both ransomware and extortion groups. However, we weren’t able to tie them to a specific group. Because there are no reporting requirements for ransomware attacks, these types of details are often left out.

Outside of the Unknown category, the LockBit ransomware group dominated ransomware attacks in 2022, accounting for 9.9% of the ransomware breach events we analyzed. LockBit rebranded itself from 2.0 to 3.0, so this figure is all inclusive of both iterations. Other groups on this list include the Hive ransomware group (7.5%), Vice Society (6.3%) and BlackCat/ALPHV (5.1%). Other, which comprises 37 other groups, collectively were responsible for 17.8% of the remaining ransomware/extortion incidents in 2022.

Despite the notorious Conti ransomware group closing up shop in May 2022, it was responsible for 5.5% of ransomware breach events we analyzed. For more information on Conti, please refer to the previous section on ransomware.

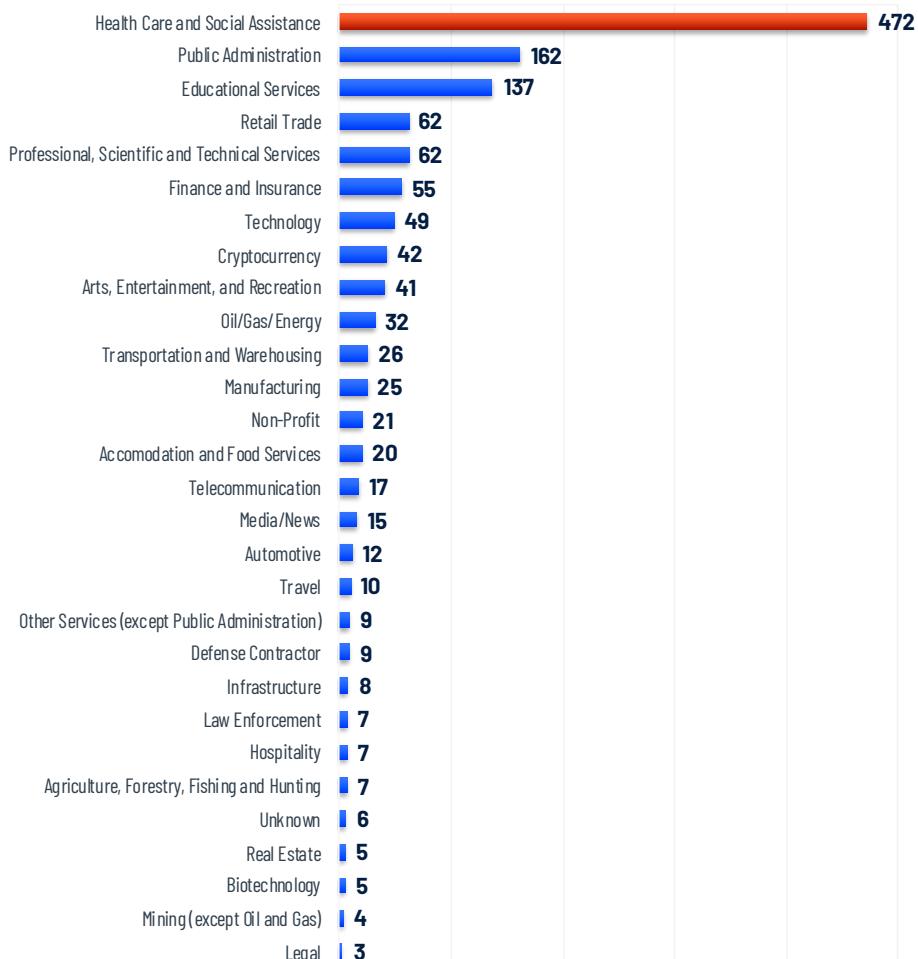
## Unspecified cyberattacks are the root cause of a quarter of breach events

We introduced a new category in 2022 called “unspecified cyberattack” as a catch-all for breach events that did not specify a type of root cause, but broadly referred to the breach event as a cyberattack or cyber incident. This category accounted for 25.2% of all breach events in 2022. More often than not, despite calling out these events as a cyberattack, many affected entities did not provide any further clarity around the incidents.

In 2022,  
healthcare  
was the  
**#1 sector**  
**targeted by**  
**ransomware**  
**attacks**  
**with 472**  
**breaches.**

Email compromise, which includes phishing attacks, accounted for 9.1% of breach events in 2022, while 5.1% were due to application misconfigurations, which commonly includes misconfigured cloud storage instances, including Amazon Simple Storage Service (S3), Google Cloud Storage Buckets and Azure Blob Storage.

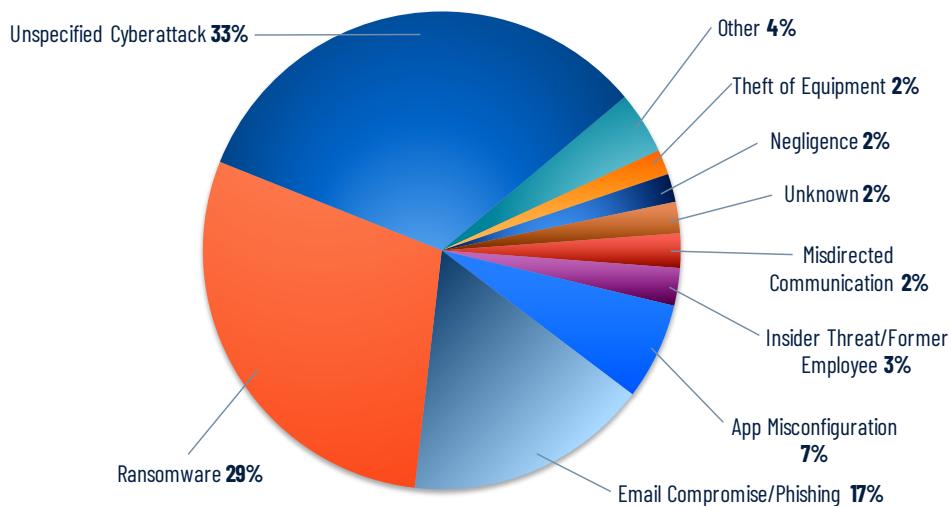
### 2022 Breaches by Industry



Unsurprisingly, healthcare and social assistance remains the industry sector with the largest number of breach events, accounting for 35.4% of all breach events we analyzed. This is a sharp increase from 2021, where 24% of breach events were attributed to healthcare.

Public administration, which includes governments, towns and municipalities, supplanted education for the number two spot in 2022, accounting for 12.1% of breach events. Educational services took the third spot in 2022, accounting for 10.3% of breach events.

## 2022 Healthcare Breaches by Root Cause

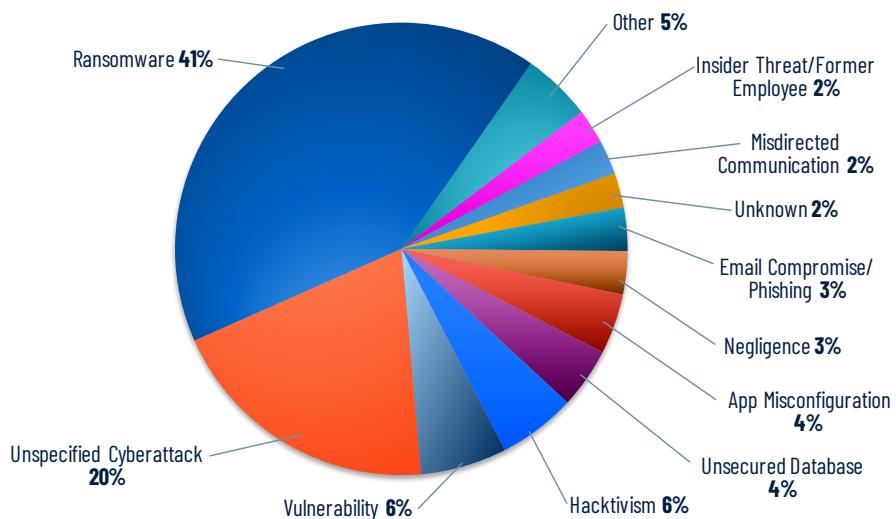


Nearly a third of all healthcare breach events we tracked in 2022 were attributed to unspecified cyberattacks, followed by ransomware at nearly 29.2%. This represents a 7% decrease compared to 2021, which saw ransomware accounting for 36.2% of healthcare breaches. In 2022, 16.5% of breaches in the healthcare sector were the result of email compromise/phishing.

## Why is healthcare the most affected industry?

Healthcare remains at the top of our breach events list each year partly because of the [reporting requirements from the U.S. Health and Human Services department](#) and its Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule (45 CFR §§ 164.400–414). Additionally, U.S. entities are required to provide a media notice if a breach event impacts more than 500 individuals. If breach reporting standards were adopted around the world and were as stringent as the HIPAA rules, perhaps we would have a lot more insight into the degree to which personally identifiable information is being exposed.

## 2022 Public Administration Breaches by Root Cause

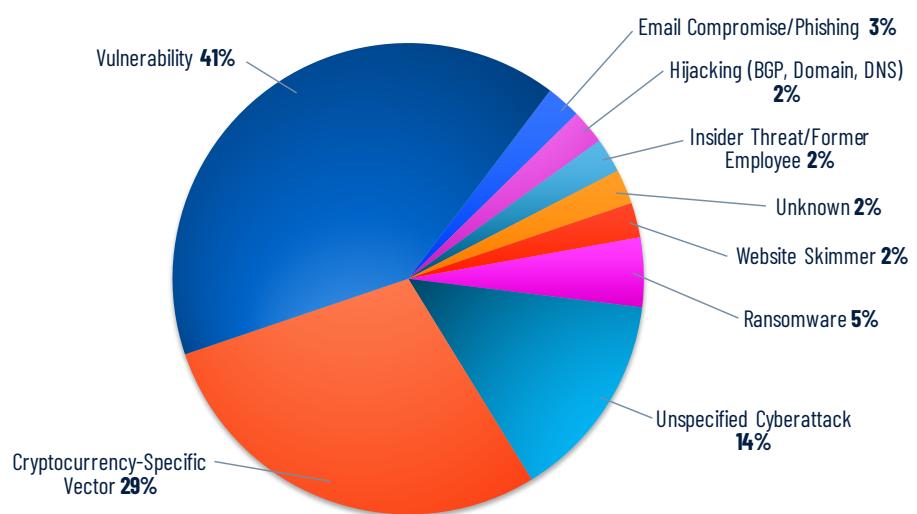


Ransomware attacks were responsible for 41.4% of all breach events in public administration. Most notably, in 2022 we observed a concerted effort to target various entities within public administration in LATAM, including Costa Rica, Brazil and Mexico. Hacktivism was also responsible for 5.6% of breach events in public administration, with a staggering 89% impacting agencies within LATAM.

## Cryptocurrency attacks resulted in the theft of \$2.4 billion dollars

In 2022, there were at least 42 breach events linked to the cryptocurrency industry, including attacks against entities in decentralized finance (DeFi), an industry in and of itself that is not managed by a central entity or corporation and is governed by code on the blockchain known as smart contracts.

**2022 Cryptocurrency Breaches by Root Cause**



Over two-thirds (69.1%) of breach events in the cryptocurrency space were the result of vulnerabilities or of a root cause we refer to as a “cryptocurrency-specific vector,” which includes things unique to this space, like **flash loan attacks** and **pricing oracle manipulation**. Over \$1.2 billion stolen in cryptocurrency breach events was attributed to these two root causes.

2022 cryptocurrency breach by root cause	Funds stolen
Vulnerability	\$766,460,000
Email compromise/phishing	\$625,000,000
Cryptocurrency-specific vector	\$531,530,000
Unspecified cyberattack	\$204,400,000
Unknown	\$160,000,000
Website skimmer	\$120,000,000
Hijacking (BGP, domain, DNS)	\$235,000
<b>Total</b>	<b>\$2,407,625,000</b>

The single largest breach event in cryptocurrency in 2022 was an attack against Sky Mavis, developers of the cryptocurrency game known as Axie Infinity. The attackers [used fake job offers over LinkedIn to steal \\$625 million from the Ronin bridge](#).

Affected entity	Funds stolen
1. Sky Mavis (Ronin)	\$625,000,000
2. Wormhole Bridge (Solana/Ethereum)	\$320,000,000
3. Bitmart	\$200,000,000
4. Beanstalk	\$182,000,000
5. Wintermute	\$160,000,000
6. Nomad	\$156,000,000
7. Badger DAO	\$120,000,000
8. Binance Bridge (BSC Chain)	\$110,000,000
9. Horizon Ethereum Bridge	\$100,000,000
10. Mango Markets	\$100,000,000

*Note: The dollar figures here are representative of the value at the time the breach events occurred, and due to the price fluctuation around various cryptocurrencies, may be cited differently across various news sources.*

For cybercriminals, breaches targeting the cryptocurrency space are likely to be their most profitable endeavors outside of ransomware.

## Understanding trends in cyberattacks through breach data

Our analysis is not an exhaustive list of every breach that may have occurred during our stated timeframe. We have observed that breaches may not be disclosed until years after they occur or are discovered, and some impacted organizations may not publicly disclose breaches at all. Therefore, we suspect the true breach figures are likely much higher than reported. However, we believe it is still practical to look at breaches that have been publicly reported in order to better understand trends from a regional and industry perspective while also diving deeper into the most common root causes of breaches.



**Known flaws remain one of the biggest risks in the vulnerability landscape**

## Conclusion

*Our examination of the vulnerability and threat landscape in 2022 yields the following lessons:*

**Addressing known vulnerabilities** is the most effective thing you can do right now. Do we sound like a broken record? Yes. We issued this same warning in 2020 and in 2021. Yet, two years later, such flaws remain one of the biggest risks in the vulnerability landscape. Unpatched vulnerabilities provide attackers with the most cost effective and straightforward way to gain initial access into or elevate privileges within organizations. Don't wait. Identify which assets in your environment are exposed to the vulnerabilities listed in this report as soon as possible.

**Ignore the hype and focus** on assessing your environment. The 2020 incident at SolarWinds and the 2021 Log4Shell vulnerability have had a lasting impact on how the industry reacts to supply chain issues. Researchers, journalists and, by extension, executives and boards are consumed with waiting for the "next Log4Shell" to drop. Instead of focusing on the branding of a vulnerability or the rumors surrounding it, organizations must examine the specific details of vulnerabilities, when available, to assess the true potential impact, rather than speculative. The key to protecting your networks is the ability to quickly appraise every facet of your environment to identify all assets and assess your code base.

**Ransomware attacks haven't slowed**, and neither should our efforts to contain them. The reports of ransomware's impending demise were greatly exaggerated. Ransomware itself is a profitable business venture for the various players in the ecosystem and we can't judge ransomware activity based solely on the entries on data leak sites. Active Directory is the key to most successful ransomware breach events, therefore organizations must harden their AD environments against ransomware attacks.

**Misconfigurations and human error** continue to pose significant risks in the cloud. With best practices guides, hardening tips and more released by CSPs, government organizations and vendors alike, ultimately it remains up to the users of cloud and container products to follow and adhere to these resources. Human errors in configuration and implementation, rather than vulnerabilities, pose some of the greatest risks in the cloud. Organizations moving to the cloud need to continuously examine their containers and deployment scripts in order to ensure their deployments meet and exceed their security thresholds. To mitigate these risks, we advise security teams to adopt cloud security posture management (CSPM) solutions. CSPM establishes a secure design and baseline configuration for assets in the cloud. By starting with a secure baseline as the building block, an organization can preemptively address concerns with user and access management and ensure that regulatory compliance is maintained as new services and environments are spun up.



## How Tenable can help

Tenable has released scan templates for Tenable One, Tenable.io Vulnerability Management, Tenable.sc, Nessus Expert and Nessus Professional, which are pre-configured to allow quick scanning for the vulnerabilities discussed in this report. In addition, Tenable One and Tenable.io Vulnerability Management customers have a new dashboard and widgets in the widgets library and Tenable.sc users also have a new dashboard covering the 2022 Threat Landscape Report.

## 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 research teams can deliver sensor coverage to our products as quickly as possible. The SRT also works to dig into technical details and author white papers, blogs, and additional communications to ensure stakeholders are fully informed of the latest risks and threats. The SRT provides breakdowns for the latest vulnerabilities on the Tenable blog.

Tenable Research has released over 180,000 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](#), Senior Manager, Research

[Satnam Narang](#), Senior Staff Research Engineer

[Ciarán Walsh](#), Associate Research Engineer

## Additional Credits:

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

[Juan Perez](#), Senior Content Marketing Manager

## About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at [tenable.com](https://www.tenable.com).

## SECTION THREE

# A Closer Look at the Key Vulnerabilities of 2022



ZERO DAY



EXPLOITED



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY



[CVE-2022-24086](#) is an improper input validation vulnerability which can lead to remote code execution (RCE) by an unauthenticated attacker. Adobe was aware of limited in-the-wild exploitation targeting Adobe Commerce merchants at the time the patch was released.



[CVE-2022-24087](#) is an improper input validation vulnerability which can lead to RCE by an unauthenticated attacker. Unlike CVE-2022-24086, CVE-2022-24087 was not found to have been exploited in the wild.



## Amazon Web Services



[CVE-2022-0070](#) and [CVE-2022-0071](#) are vulnerabilities in the Apache Log4j Hot Patch Service produced by Amazon Web Services caused by the ability to execute commands with unnecessary privileges.



**NO-CVE-ID:** A XML External Entity (XXE) vulnerability found in the AWS CloudFormation service. When exploited, the vulnerability allows attackers to get file and credential disclosure primitives which can be used to leak sensitive files in vulnerable machines.

**Name:** [BreakingFormation](#)



**NO-CVE-ID:** An information disclosure vulnerability in AWS Glue. When the vulnerability is exploited, the attacker can access credentials for AWS service accounts, giving them full access to the internal service API. Combining this exploit with a misconfiguration in the API, attackers are able to escalate privileges to unrestricted access to all resources in the region.

**Name:** [Superglue](#)



## Apache



[CVE-2021-31805](#) is a forced Object-Graph Navigation Language (OGNL) evaluation vulnerability in Apache Struts that may lead to RCE. This is a secondary fix for CVE-2020-17530 because the initial patch was incomplete.



[CVE-2021-44228](#) is a RCE vulnerability in Apache Log4j 2. An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted request to a server running a vulnerable version of log4j. The crafted request uses a Java Naming and Directory Interface (JNDI) injection via a variety of services including:

- Lightweight Directory Access Protocol
- Secure LDAP
- Remote Method Invocation
- Domain Name Service

If the vulnerable server uses Log4j to log requests, the exploit will then request a malicious payload over JNDI through one of the services above from an attacker-controlled server. Successful exploitation could lead to RCE.

**Name: Log4Shell**



[CVE-2021-44521](#) is a code injection vulnerability in Apache Cassandra. In order to exploit this vulnerability, certain non-default configuration requirements are needed. Successful exploitation would allow an attacker to escape the sandbox and achieve RCE.



[CVE-2022-42889](#) is an unsafe script evaluation vulnerability in the default interpolators in the Apache Commons Text StringSubstitutor class. An attacker can exploit this vulnerability by passing a specially crafted string containing untrusted data, commonly through a user input field, that is interpolated by the StringSubstitutor class. Successful exploitation would result in arbitrary code execution or cause an application to perform arbitrary lookup to an attacker controlled remote server.

**Name: Text4Shell**



## Apple



[CVE-2021-1789](#) is a type confusion vulnerability in iOS, iPadOS, macOS, tvOS and watchOS. A vulnerable device that visits or processes a specially crafted web page could grant an attacker arbitrary code execution privileges. According to Google's Threat Analysis Group (TAG), this vulnerability was [exploited in the wild as part of an attack chain](#) that includes CVE-2021-30869.



[CVE-2021-30869](#) is a type confusion vulnerability in iOS, iPadOS and macOS. A malicious application containing exploit code could gain arbitrary code execution with kernel privileges.



## Apple Continued >>

[\*\*CVE-2022-22587\*\*](#) is a memory corruption issue in the IOMobileFrameBuffer in macOS, iOS and iPadOS. A malicious application could exploit the flaw to gain arbitrary code execution with kernel privileges.



[\*\*CVE-2022-22588\*\*](#) is a resource exhaustion issue in iOS and iPadOS. An attacker could exploit this vulnerability when an iOS or iPadOS device tries to process a maliciously named HomeKit accessory. Successful exploitation could lead to a denial of service (DoS) condition.

**Name:** doorLock



[\*\*CVE-2022-22594\*\*](#) is a cross-origin issue in the IndexDB API for WebKit Storage. Exploitation of this flaw would allow a website to track sensitive user information.



[\*\*CVE-2022-22620\*\*](#) is a use after free vulnerability issue affecting macOS, iOS and iPadOS. A malicious website could be used to gain arbitrary code execution. Apple was aware of in-the-wild exploitation of this flaw at the time the patch was released.



[\*\*CVE-2022-22674\*\*](#) is an out-of-bounds read issue in the Intel Graphics Driver for macOS. An attacker could exploit this vulnerability to read memory from the kernel.



[\*\*CVE-2022-22675\*\*](#) is an out-of-bounds write vulnerability in AppleAVD in macOS and watchOS that was exploited in the wild. An attacker could exploit this vulnerability by using a specially crafted application to read kernel memory.



[\*\*CVE-2022-32893\*\*](#) is an out-of-bounds write issue in Apple's WebKit web browser engine in iOS, iPadOS and macOS. An attacker could exploit this vulnerability by socially engineering a target into visiting a website containing malicious web content. Successful exploitation could result in arbitrary code execution.



[\*\*CVE-2022-32894\*\*](#) and [\*\*CVE-2022-32917\*\*](#) are out-of-bounds write issues in the iOS, iPadOS and macOS kernel. An attacker could exploit this flaw by convincing a victim to open a specially crafted application containing malicious code. Successful exploitation could result in arbitrary code execution with kernel privileges.



[\*\*CVE-2022-42827\*\*](#) is an out-of-bounds write vulnerability affecting the iOS and iPadOS kernel which could allow arbitrary code execution with kernel privileges.



## Apple Continued >>

[CVE-2022-42856](#) is a type confusion vulnerability in Apple's WebKit web browser engine in macOS, iOS, iPadOS, tvOS and Safari. An attacker could exploit this vulnerability by socially engineering a target into visiting a website containing malicious web content. Successful exploitation could result in arbitrary code execution.



## Arm

[CVE-2022-23960](#) is a cache speculation vulnerability where malicious code uses the shared branch history to influence mispredicted branches within the victim's hardware. This technique can be used to cause cache allocation, which allows an attacker to access data that should not be accessible.

**Name: Spectre-BHB**



## Atlassian

[CVE-2022-26134](#) is an OGNL injection vulnerability in Atlassian Confluence Server and Data Center. An unauthorized, remote attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable Confluence Server or Data Center instance. Successful exploitation would result in arbitrary code execution.



[CVE-2022-26136](#) is an arbitrary servlet filter bypass vulnerability in multiple Atlassian products. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted HTTP request to bypass a variety of Servlet filters used by first- and third-party applications.



[CVE-2022-26137](#) is a servlet filter invocation vulnerability in multiple Atlassian products. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted HTTP request to bypass the servlet filter used to respond to Cross-Origin Resource Sharing (CORS) requests.



[CVE-2022-26138](#) is a hardcoded password vulnerability in the Questions for Confluence App for Confluence Server and Confluence Data Center. The application creates a default user account with elevated privileges. An attacker with knowledge of the hardcoded password could exploit the flaw to gain access to Confluence and access any pages that the 'confluence-users' group has access to.



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



NOTEWORTHY

## Cisco



[CVE-2020-3153](#) is an uncontrolled search path vulnerability in the Cisco AnyConnect Secure Mobility Client for Windows. An authenticated, local attacker with valid Windows credentials could exploit this vulnerability using a malicious file copied to a system directory. Successful exploitation would allow an attacker to copy the malicious files to locations on the Windows system that have system level privileges.



[CVE-2020-3433](#) is a DLL hijacking vulnerability in the Cisco AnyConnect Secure Mobility Client for Windows. An authenticated, local attacker with valid Windows credentials could exploit this vulnerability through a specially crafted IPC message to the AnyConnect process. Successful exploitation would grant arbitrary code execution privileges as SYSTEM.



[CVE-2022-20624](#) is a DoS vulnerability in the Cisco Fabric Services over IP (CFSoIP) feature found in Cisco's NX-OS software. An unauthenticated, remote attacker could exploit the flaw by sending specially crafted CFSoIP packets to a vulnerable device. Successful exploitation would result in a DoS condition.



[CVE-2022-20821](#) is an open port vulnerability in the Cisco IOS XR software health check remote patient monitor. An unauthenticated, remote attacker could exploit the flaw by connecting to the Redis instance over the open port and write to the in-memory database or container filesystem and retrieve database information.



## Citrix



[CVE-2019-19781](#) is a directory traversal vulnerability in the Citrix Application Delivery Controller (ADC) and Gateway product. 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. It was featured as one of the top five vulnerabilities in the 2020 Threat Landscape Retrospective.



[CVE-2022-27510](#) is an authentication bypass vulnerability in Citrix ADC and Gateway. It was assigned a CVSSv3 score of 9.8 and is labeled as Critical. In its bulletin, Citrix noted that this vulnerability affects appliances that have enabled secure socket layer virtual private network (SSL VPN) functionality or are being used as an Independent Computing Architecture Proxy with authentication. Authentication bypass vulnerabilities like this one could be exploited by an attacker as an initial access vector into a network



## Citrix Continued >>

[CVE-2022-27518](#) is a RCE vulnerability impacting Citrix ADC or Citrix Gateway when configured as a Security Assertion Markup Language (SAML) service provider (SP) or a SAML identity provider (IdP). The vulnerability is rated as critical and can be exploited by a remote, unauthenticated attacker to execute arbitrary code. CVE-2022-27518 was given a CVSSv3 score of 9.8.



## F5



[CVE-2020-5902](#) is a critical directory traversal vulnerability in the traffic management user interface (TMUI) of the BIG-IP product line, which includes a variety of solutions both software and hardware-based. An unauthenticated, remote attacker could send a specially crafted request to a vulnerable BIG-IP device containing a directory traversal character sequence (e.g. “..;/”) to exploit the vulnerability. Successful exploitation would give an attacker the ability to execute arbitrary system commands, create or delete files, or disable services on the vulnerable host. It was featured as one of the top five vulnerabilities in the 2020 Threat Landscape Retrospective.



[CVE-2022-1388](#) is an authentication bypass vulnerability in the REST component of BIG-IP's iControl API that was assigned a CVSSv3 score of 9.8. The iControl REST API is used for the management and configuration of BIG-IP devices. CVE-2022-1388 could be exploited by an unauthenticated attacker with network access to the management port or self IP addresses of devices that use BIG-IP. Exploitation would allow the attacker to execute arbitrary system commands, create and delete files and disable services.



## Fortinet



[CVE-2018-13379](#) is an unauthenticated information disclosure vulnerability in FortiOS SSL VPNs. This arbitrary file read vulnerability 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.



[CVE-2022-40684](#) is a critical authentication bypass vulnerability that received a CVSSv3 score of 9.6. By sending specially crafted HTTP or HTTPS requests to a vulnerable target, a remote attacker with access to the management interface could perform administrator operations.



ZERO DAY



EXPLOITED



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY



## Fortinet Continued >>

[CVE-2022-42475](#) is a heap-based buffer overflow in several versions of FortiOS that received a CVSSv3 score of 9.3. A remote, unauthenticated attacker could exploit this vulnerability with a specially crafted request and gain code execution.



## Google

[CVE-2021-22600](#) and [CVE-2021-39793](#) are elevation of privilege (EoP) vulnerabilities in Google's Upstream Kernel for Android. It was assigned a severity score of Moderate. According to Google, these vulnerabilities have been under limited, targeted exploitation.



[CVE-2022-0609](#) is a use-after-free vulnerability in the Animation engine of Google Chrome. It was reported by Google's Threat Analysis Group and has been exploited in the wild.



[CVE-2022-1096](#) is a type confusion vulnerability in the V8 engine for Google Chrome. It was reported by Anonymous and has been exploited in the wild.



[CVE-2022-1364](#) is a type confusion vulnerability in the V8 engine for Google Chrome. It was reported by Google's Threat Analysis Group and has been exploited in the wild.



[CVE-2022-2294](#) is a heap-based buffer overflow vulnerability in the Web Real-Time Communications (WebRTC) component of Chromium.



[CVE-2022-2856](#) is an improper input validation vulnerability in Google Chrome. This vulnerability was reported by Google's Threat Analysis Group as having been exploited in the wild.



[CVE-2022-3075](#) is an insufficient data validation vulnerability in the Mojo IPC system in Google Chrome. The vulnerability was reported by an Anonymous researcher and confirmed to have been exploited in the wild.



## Google Continued >>

[CVE-2022-3723](#) is a type confusion vulnerability in the V8 engine for Google Chrome. It was reported by researchers at Avast and has been exploited in the wild.



[CVE-2022-4135](#) is a heap buffer overflow vulnerability in Google Chrome's GPU. It was reported by Google's Threat Analysis Group and has been exploited in the wild.



[CVE-2022-4262](#) is a type confusion vulnerability in the V8 engine for Google Chrome. It was reported by Google's Threat Analysis Group and has been exploited in the wild.



## Magnitude Simba



[CVE-2022-29972](#) is an improper validation of authentication token vulnerability in the Magnitude Simba Amazon Redshift ODBC and JDBC drivers. A local, authenticated attacker could exploit this vulnerability to execute remote commands.

Name: SynLapse



## Microsoft



[CVE-2017-11882](#) is a memory corruption vulnerability in the Equation Editor component of Microsoft Office that could lead to RCE and received a CVSSv3 score of 7.8. It has been exploited in attacks by diverse threat actors and is incorporated into some of the top malware strains.



[CVE-2018-0798](#) is a memory corruption vulnerability in the Equation Editor component of Microsoft Office that could lead to RCE and received a CVSSv3 score of 8.8. Exploitation could allow arbitrary code execution in the context of the user who interacted with a specially crafted file or website.



[CVE-2018-0802](#) is a memory corruption vulnerability in the Equation Editor component of Microsoft Office that could lead to RCE and received a CVSSv3 score of 8.6. Exploitation could allow arbitrary code execution in the context of the user who interacted with a specially crafted file or website.



## Microsoft Continued >>

---

[CVE-2020-0688](#) is a validation key vulnerability due to the generation of static cryptographic keys that could lead to RCE. The vulnerability was reported to the Zero Day Initiative and was subsequently disclosed to Microsoft. Soon after the vulnerability was disclosed in 2020, reports began to emerge that threat actors were utilizing the flaw in the wild.



[CVE-2020-1472](#) is an EoP vulnerability in Microsoft's Netlogon Remote Protocol. This protocol is used to maintain relationships of domain controllers (DCs) within and across domains. Critically, MS-NRPC is also used to manage account changes for DCs, like passwords. The flaw exists because of a flaw in how MS-NRPC implements AES-CFB8 encryption. Because this is a local privilege escalation flaw, an attacker needs to be on the same local area network as their target. Active Directory is a target of serious concern with Zerologon. If an attacker was able to exploit it against AD, they could impersonate any machine on the network, reset the domain controller's administrator password or launch ransomware attacks against the entire network.

**Name: Zerologon**



[CVE-2021-26855](#) is a server-side request forgery (SSRF) vulnerability dubbed ProxyLogon by Orange Tsai, the researcher credited with its discovery. An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted HTTP request to a vulnerable Exchange Server that accepts untrusted connections over port 443. Successful exploitation of this flaw would allow the attacker to authenticate to the targeted Exchange Server. It was featured as one of the top five vulnerabilities in the 2021 Threat Landscape Retrospective.

**Name: ProxyLogon**



[CVE-2021-26857](#) is an insecure deserialization vulnerability. Specifically, the flaw resides in the Exchange Unified Messaging Service, which enables voicemail functionality in addition to other features. To exploit this flaw, an attacker would need to be authenticated to the vulnerable Exchange Server with administrator privileges, potentially by exploiting another vulnerability first. Successful exploitation would grant the attacker arbitrary code execution privileges as SYSTEM.



[CVE-2021-26858](#) and [CVE-2021-27065](#) are arbitrary file write vulnerabilities. These flaws are post-authentication, meaning an attacker would first need to authenticate to the vulnerable Exchange Server before they could exploit them. This could be achieved by exploiting CVE-2021-26855 or by using stolen administrator credentials. Once authenticated, an attacker could arbitrarily write to any paths on the vulnerable server.



[CVE-2021-34473](#), a RCE vulnerability; [CVE-2021-34523](#), an EoP vulnerability; and [CVE-2021-31207](#), a feature bypass make up the vulnerability chain named ProxyShell. By chaining these vulnerabilities, an attacker could execute arbitrary commands on vulnerable Exchange servers on port 443.

**Name: ProxyShell**



## Microsoft Continued >>

---

[\*\*CVE-2021-36942\*\*](#) is a Windows Local Security Authority (LSA) Spoofing Vulnerability that was patched in August in relation to the PetitPotam NTLM relay attack disclosed by Gilles Lionel. The exploit could be used to force domain controllers to authenticate with an attacker-controlled destination. Roughly a month after disclosure, ransomware groups were seen exploiting this attack. The patch for CVE-2021-36942 only partially patched the issue. Microsoft published general mitigation guidance for [defending against NTLM Relay Attacks](#). The LockFile ransomware has chained Microsoft Exchange vulnerabilities with PetitPotam to take over domain controllers.

Name: PetitPotam



---

[\*\*CVE-2021-40444\*\*](#) is a RCE vulnerability in Microsoft's MSHTML (Trident) platform, Microsoft's proprietary browser engine. To exploit this vulnerability, an attacker would need to create a specially crafted Microsoft Office document containing a malicious ActiveX control and use social engineering techniques to convince their target to open the document. The impact of this vulnerability would be more significant in cases where the recipient has administrative privileges.



---

[\*\*CVE-2022-21836\*\*](#) is a spoofing vulnerability affecting Windows certificates which has received a 7.8 CVSSv3 score. An attacker could utilize compromised certificates to bypass the Windows Platform Binary Table binary verification. While exploitation is rated as less likely, Microsoft states that the flaw was publicly disclosed. The compromised certificates known to Microsoft have been added to the Windows kernel driver block list and Microsoft offers additional guidance in its security advisory.



---

[\*\*CVE-2022-21839\*\*](#) is an uncontrolled resource consumption vulnerability in the Windows Event Tracing Discretionary Access Control List. A local attacker could exploit this vulnerability to cause a DoS condition.



---

[\*\*CVE-2022-21874\*\*](#) is a RCE in the Windows Security Center API that received a CVSSv3 score of 7.8. This vulnerability requires user interaction to exploit and the attack vector is local.



---

[\*\*CVE-2022-21882\*\*](#) is an EoP vulnerability in the Win32k system driver. A local, authenticated attacker could exploit this vulnerability to elevate privileges.



---

[\*\*CVE-2022-21907\*\*](#) is a RCE vulnerability in the Internet Information Services component of Microsoft operating systems: Windows 10, Windows Server 2022 and Windows Server 2019. The vulnerability can be exploited by sending a specially crafted HTTP request to a vulnerable target, leading to a DoS which may be chained with other vulnerabilities leading to RCE.



## Microsoft Continued >>

---

[\*\*CVE-2022-21919\*\*](#) is an EoP vulnerability in the Windows User Profile Service. To exploit this vulnerability, an attacker would need to have established a foothold on the vulnerable system through social engineering, a separate exploit or malware. Successful exploitation would give an attacker elevated privileges on the vulnerable system.



[\*\*CVE-2022-21971\*\*](#) is a RCE vulnerability in Windows Runtime. An attacker could exploit this vulnerability by convincing a target to open a specially crafted document file containing malicious code. Successful exploitation would grant the attacker arbitrary code execution privileges.



[\*\*CVE-2022-21989\*\*](#) is an EoP vulnerability in the Windows Kernel. According to Microsoft Exploitability Index rating, this vulnerability is more likely to be exploited. The advisory noted that an attacker needs to take additional actions prior to exploitation of this vulnerability, which is evident by the "High" rating for "Attack Complexity" in the CVSSv3 score of 7.8.



[\*\*CVE-2022-21990\*\*](#) is a RCE vulnerability in Microsoft's Remote Desktop Client. To exploit the flaw, an attacker would need to convince a user to connect to an attacker-controlled Remote Desktop server.



[\*\*CVE-2022-22047\*\*](#) is an EoP vulnerability in the Windows Client Server Run-Time Subsystem. This type of vulnerability is likely to have been used as part of post-compromise activity, once an attacker has gained access to the targeted system and run a specially crafted application.



[\*\*CVE-2022-22713\*\*](#) is a DoS vulnerability impacting Windows Hyper-V. According to Microsoft's description, exploitation of the vulnerability requires an attacker to win a race condition giving it a high complexity rating and a CVSSv3 score of 5.6. It was publicly disclosed prior to a patch being available.



[\*\*CVE-2022-24459\*\*](#) is an EoP vulnerability affecting the Windows Fax and Scan service. The vulnerability carries a CVSSv3 score of 7.8 and can be exploited by a local, authenticated attacker. While the severity and requirements for exploitation would typically be less concerning, this vulnerability was publicly disclosed.



[\*\*CVE-2022-24512\*\*](#) is a RCE vulnerability in Microsoft .NET and Visual Studio. According to Microsoft, exploitation of this flaw requires that "a user trigger the payload in the application."



ZERO DAY



EXPLOITED



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY

## Microsoft Continued >>

---

[\*\*CVE-2022-24521\*\*](#) is an EoP vulnerability in the Windows Common Log File System Driver. An attacker that has already gained access to a vulnerable system could exploit this vulnerability by running a specially crafted application. Successful exploitation would give the attacker the ability to run processes in an elevated context.



[\*\*CVE-2022-26809\*\*](#) is a critical RCE vulnerability in the Remote Procedure Call (RPC) runtime. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted RPC call to a host.



[\*\*CVE-2022-26904\*\*](#) is an EoP vulnerability in the Windows User Profile service. The attack complexity for this flaw is considered high because it requires an attacker to win a race condition. Successful exploitation would allow an attacker to gain privileged access for a lower privileged account.



[\*\*CVE-2022-26923\*\*](#) is an EoP vulnerability in Microsoft Active Directory Certificate Services (AD CS). An attacker with low privileges on a vulnerable system with AD CS running could exploit this by running a specially crafted script. Successful exploitation would allow the attacker to elevate from a low-privileged user to domain administrator.



[\*\*CVE-2022-26925\*\*](#) is a spoofing vulnerability in the Windows LSA that was exploited in the wild. An unauthenticated attacker could coerce domain controllers to authenticate to an attacker-controller server using NTLM.



[\*\*CVE-2022-30137\*\*](#) is an EoP vulnerability in Microsoft Azure Service Fabric for Linux. A local, authenticated attacker could exploit the vulnerability to escalate privileges to gain root privileges on a node. Successful exploitation could potentially result in the compromise of all of the nodes within a cluster.

**Name: FabricScape**



[\*\*CVE-2022-30190\*\*](#) is a RCE vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT) that impacts several versions of Microsoft Office, including patched versions of Office 2019 and 2021. The vulnerability exists due to the way Microsoft Windows Support Diagnostic Tool (MSDT) is called using the URL protocol from certain applications. Because of the way this vulnerability is exploited, Microsoft lists the attack vector as "local," but an attacker leveraging this flaw would likely be remote.

**Name: Follina**



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY

## Microsoft Continued >>

---

[\*\*CVE-2022-30216\*\*](#) is an authentication coercion vulnerability in Microsoft Windows Server due to an off-by-one error found in a procedure of the security callback. According to researchers, an attacker could exploit this vulnerability by combining it with a New Technology LAN Manager (NTLM) relay attack against AD CS.



[\*\*CVE-2022-33675\*\*](#) is an EoP vulnerability in the Microsoft Azure Site Recovery Suite. The cause of the vulnerability is incorrect permissions in one of the software's installation folders. An attacker could leverage this vulnerability by hijacking DLLs stored in this folder, leading to malicious code running with SYSTEM privileges.



[\*\*CVE-2022-34713\*\*](#) is a RCE vulnerability in MSDT. An attacker could exploit this flaw by using social engineering to convince a target to open a malicious document or open a link that downloads a malicious file. It was first disclosed by researcher Imre Rad in January 2020. Following the discovery of the Follina vulnerability (CVE-2022-30190), Microsoft re-evaluated Rad's findings and patched this flaw.

**Name:** DogWalk



[\*\*CVE-2022-37969\*\*](#) is an EoP vulnerability in the Windows Common Log File System Driver. According to Microsoft, this vulnerability has been exploited in the wild and has been publicly disclosed prior to a patch being available. This is a post-exploitation vulnerability, meaning it can be exploited after an attacker has gained access to a vulnerable target system via other means, including exploiting a separate vulnerability or through social engineering.



[\*\*CVE-2022-37981\*\*](#) is a DoS vulnerability in the Microsoft Windows Event Logging Service. According to Microsoft, the availability is set to Low on this flaw because while performance can be interrupted and/or reduced, "the vendor advisory noted that an attacker "cannot fully deny service."

**Name:** OverLog



[\*\*CVE-2022-41033\*\*](#) is an EoP vulnerability in the Windows COM+ Event System Service, which enables system event notifications for COM+ component services. An authenticated attacker could exploit this vulnerability to elevate privileges on a vulnerable system and gain SYSTEM privileges.



[\*\*CVE-2022-41040\*\*](#) is a SSRF vulnerability in Microsoft Exchange Server. An authenticated attacker could exploit this vulnerability by leveraging stolen credentials for any Exchange Server user account.

**Name:** ProxyNotShell



## Microsoft Continued >>

---

[\*\*CVE-2022-41043\*\*](#) is an information disclosure vulnerability in Microsoft Office for Mac. Exploitation of this flaw requires an attacker to have gained local access to the vulnerable host. It was publicly disclosed prior to a patch being made available.



[\*\*CVE-2022-41073\*\*](#) is an EoP vulnerability affecting the Windows Print Spooler service. The vulnerability carries a CVSSv3 score of 7.8 and discovery was credited to Microsoft Threat Intelligence Center. This flaw has been exploited in the wild, according to Microsoft, and could allow a low privileged user to gain SYSTEM level privileges.



[\*\*CVE-2022-41082\*\*](#) is a RCE vulnerability. An authenticated attacker could exploit this vulnerability by leveraging stolen credentials for any Exchange Server user account. It can be chained together with CVE-2022-41040.

**Name:** ProxyNotShell



[\*\*CVE-2022-41091\*\*](#) is a security feature bypass vulnerability affecting Windows Mark of the Web (MoTW). MoTW is a security feature used to tag files downloaded from the internet and prevent them from performing certain actions. Files flagged with MoTW would be opened in Protected View in Microsoft Office — prompting users with a security warning banner asking them to confirm the document is trusted by selecting Enable content. A malicious actor could craft a file that could bypass MoTW, “resulting in a limited loss of integrity and availability of security features such as Protected View.”



[\*\*CVE-2022-41125\*\*](#) is an EoP vulnerability in the Windows Cryptography Next Generation (CNG) Key Isolation Service used for Windows cryptographic support and operations. With a CVSSv3 score of 7.8, successful exploitation would allow an attacker to gain SYSTEM privileges



[\*\*CVE-2022-41128\*\*](#) is a critical vulnerability impacting the JScript9 scripting language in Windows operating systems. The vulnerability can be used to drop malware on a target by directing the user to navigate to a malicious website that exploits the weakness.



[\*\*CVE-2022-44698\*\*](#) is a security feature bypass vulnerability in the Windows operating system. MoTW vulnerability that prevents specially crafted downloads from being marked as being from the web, which affects the integrity and availability of security features that utilize MoTW tagging. Successful exploitation prevents SmartScreen from performing a reputation check on the downloaded file. This could lead to a known malicious executable not alerting users that the file may be malicious.



## Microsoft Continued >>

**NO-CVE-ID:** A critical cross-account vulnerability was discovered in Azure Automation service. No CVE identifier was assigned for this vulnerability. An unauthorized user could send a specially crafted request to a special identity endpoint and obtain tokens belonging to other users/organizations.

**Name:** AutoWarp



**NO-CVE-ID:** A cross-account authentication bypass vulnerability using a forged certificate was discovered in Microsoft Azure's PostgreSQL engine. When chained with a privilege escalation vulnerability, an attacker could gain unauthorized access to read other customers' PostgreSQL databases.

**Name:** #ExtraReplica



**NO-CVE-ID:** A privilege escalation vulnerability was discovered in Microsoft Azure's PostgreSQL engine. When chained with a cross-account authentication bypass vulnerability, an attacker could gain unauthorized access to read other customers' PostgreSQL databases.

**Name:** #ExtraReplica



## Mitel



[CVE-2022-29499](#) is an improper input validation vulnerability in MiVoice Connect, a component of the Mitel Service Appliance. An unauthenticated, remote attacker could exploit this vulnerability to gain RCE privileges within the context of the Service Appliance.



## Mozilla



[CVE-2022-26485](#) is a use-after-free vulnerability in Mozilla Firefox in the way that parameters are processed through Extensible Stylesheet Language Transformations (XSLT). When an XSLT parameter is removed during processing, it could result in an exploitable use-after-free. Mozilla said it has received reports that this flaw has been exploited in the wild.



[CVE-2022-26486](#) is a use-after-free vulnerability in Mozilla Firefox in the WebGPU IPC framework. Use-after-free and sandbox escape is possible when the framework receives an unexpected message. Mozilla said it has received reports that this flaw has been exploited in the wild.





## Nooie

**NO-CVE-ID:** Nooie Baby Monitors contain multiple vulnerabilities, including an unauthenticated message queue telemetry transport information leak, an unauthorized access vulnerability in the real time streaming protocol and a missing access control policy for an AWS bucket. These three vulnerabilities were not assigned a CVE identifier but have allowed an outside attacker to access the Baby Monitor camera or further compromise the vulnerable device through malicious code execution.



## Okta

[CVE-2022-24295](#) is a command injection vulnerability in Okta Advanced Server Access Client for Windows. Successful exploitation of this vulnerability could give an attacker RCE privileges.



## Open Source

### Argo CD



[CVE-2022-24348](#) is a path traversal vulnerability in Argo CD. In order to exploit this flaw, an attacker with permissions to create or update Applications that can either guess or has knowledge of the full path to a file containing valid YAML, could create a malicious Helm chart to consume YAML as value files.



### CRI-O



[CVE-2022-0811](#) is a vulnerability in CRI-O v1.19 container runtime. For this vulnerability to be exploited, the attacker must have rights to deploy a pod on a Kubernetes cluster. When exploited, it allows for container escape and gaining root access on the host, letting the attacker move freely in the cluster.

Name: cr8escape



### Horde Webmail

**NO-CVE-ID:** Horde Webmail contains a stored cross-site scripting (XSS) vulnerability that was not assigned a CVE identifier. To exploit this flaw, an attacker can send a specially crafted email to a user using a vulnerable version of Horde Webmail. Even if they preview the email, the exploit will be triggered.





## Linux Kernel

[CVE-2021-3995](#) is a flaw in the libmount library of util-linux. When leveraged, this flaw could allow unmounting of certain FUSE filesystems by unprivileged, local attackers. Target filesystems must be owned by other users whose UID is a prefix of the attacker's UID when in string form. Exploitation of this flaw may cause DoS to applications using these filesystems.



[CVE-2021-3996](#) is a flaw in the libmount library of util-linux. When leveraged, this flaw could allow unmounting of certain FUSE filesystems by unprivileged, local attackers. Target filesystems must be world-writable or in a world-writable directory. Exploitation of this flaw may cause DoS to applications using these filesystems.



[CVE-2021-3997](#) is an uncontrollable recursion flaw in systemd-tmpfiles. The flaw can cause a DoS when too many directories are created in /tmp at boot time.



[CVE-2021-3998](#) is a flaw in the realpath() function of glibc that can cause information leakage or sensitive data disclosure.



[CVE-2021-3999](#) is an off-by-one buffer overflow and underflow vulnerability in glibc. If the buffer size is 1, a local attacker could leverage the vulnerability to execute arbitrary code or elevate their privileges.



[CVE-2022-0185](#) is a heap-based buffer overflow found in the Filesystem Context functionality of the Linux kernel. When exploited, this vulnerability can lead to an unprivileged user escalating their privileges.



[CVE-2022-0492](#) is an improper authentication vulnerability in the Linux kernel. It requires specific configuration to facilitate exploitation, which could allow an attacker to escape a container and escalate privileges.



[CVE-2022-0847](#) is an improper initialization vulnerability in the Linux kernel. The flaw resides in the new pipe\_buffer, which can lead to the improper preservation of permissions.

**Name: DirtyPipe**



[CVE-2022-29799](#) is a directory traversal vulnerability found in the networkd-dispatcher unit of the Linux kernel. The cause of the vulnerability is the lack of function sanitization by the OperationalState and AdministrativeState networkd-dispatcher leading to escape from the "/etc/networkd-dispatcher" directory.

**Name: NimbusPwn**



ZERO DAY



EXPLOITED



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY

## Open Source/Linux Kernel Continued >>

---

[CVE-2022-29800](#) is a time-of-check-time-of-use race condition vulnerability in the networkd-dispatcher unit of the Linux kernel. The vulnerability can be exploited by replacing scripts used by the unit between the time they are discovered and the time they are run, leading networkd-dispatcher to believe the attacker-controlled scripts are owned by root.

**Name:** NimbusPwn



## OpenSSL



[CVE-2022-3602](#) is a buffer overflow vulnerability in OpenSSL caused by a function that verifies x.509 certificates.

Preannounced as a critical vulnerability, this rating was later downgraded to “high” after it was determined that it would not likely cause RCE. However it is still possible that when exploited in uncommon environments to achieve RCE.



[CVE-2022-3786](#) is a buffer overflow vulnerability in OpenSSL caused by a function that verifies x.509 certificates. As the attacker cannot control overflowed data, but only the length of data passed to the function, it is unlikely that this vulnerability will lead to RCE if exploited.



## PrestaShop



PrestaShop

[CVE-2022-31181](#) is a SQL injection vulnerability in PrestaShop CMS. According to developers, it is used as part of a “previously unknown vulnerability chain” to gain RCE on PrestaShop installations.



## Redis



[CVE-2022-0543](#) is a vulnerability in Redis on Debian-specific (Debian, Ubuntu) distributions of Linux that use the Lua engine. An attacker could exploit this vulnerability to escape the Lua sandbox to achieve RCE.



## WSO2



[CVE-2022-29464](#) is an unrestricted arbitrary file upload vulnerability in various WSO2 products. An unauthenticated, remote attacker could exploit the vulnerability by uploading a specially crafted Jakarta Server Pages file to a vulnerable server.



## SQLite



[CVE-2022-35737](#) is an improper validation of array index vulnerability in SQLite. The vulnerability impacts applications using SQLite’s Library API. It can be exploited when passing large string inputs (2GB, for example) to an application or program using a vulnerable version of SQLite that uses printf functions.



## Oracle



[CVE-2020-14882](#) is an unauthenticated RCE flaw in the console component of Oracle WebLogic Server. Oracle described the flaw as easily exploitable and assigned it a CVSSv3 score of 9.8. Successful exploitation would allow an unauthenticated attacker to compromise the Oracle WebLogic server over HTTP and take complete control of the host.



[CVE-2022-21500](#) is a vulnerability within Oracle E-Business Suite 12.2 which allows an unauthenticated attacker with network access to access critical data. Authentication is required for a successful attack, however the user may be self-registered.



## Palo Alto Networks



[CVE-2022-0028](#) is a reflected amplification DoS vulnerability in the Palo Alto Networks PAN-OS URL filtering policy due to a misconfiguration. An attacker could exploit this flaw to perform a DoS attack that would obfuscate the source of the attack, making it appear as though it was originating from a Palo Alto Networks device, such as its PA-Series (hardware), VM-Series (virtual) or CN-Series (container) firewall.



## PolKit



PolKit

[CVE-2021-4034](#) is an EoP vulnerability in PolKit's pkexec, a command line tool included in most Linux distributions by default. Successful exploitation would give an unprivileged, local attacker root privileges on the vulnerable system.

Name: PwnKit



## PTC



[CVE-2022-25246](#) is a hard-coded credentials vulnerability in the UltraVNC installation of Axeda products. The affected products are Axeda agent and Axeda Desktop Server for Windows. If exploited, this vulnerability can lead to RCE on the target machine.

Name: Access:7



ZERO DAY



EXPLOITED



NAMED VULNERABILITY



PRE-2022 VULNERABILITY



CLOUD



NOTEWORTHY

[\*\*CVE-2022-25247\*\*](#) is a RCE vulnerability found in Axeda agent and Axeda Desktop Server for Windows. If leveraged, an attacker can send certain commands to a specific port, without authentication. This can then lead to full file system access and RCE.

**Name: Access:7**



[\*\*CVE-2022-25248\*\*](#) is an information disclosure vulnerability in the ERemoteServer.exe service of Axeda Agent and Axeda Desktop Server For Windows products. When an attacker connects to a specific port on a target running these products, the products return the event log for the specific service associated with that port.

**Name: Access:7**



[\*\*CVE-2022-25249\*\*](#) is a directory traversal vulnerability in Axeda Agent and Axeda Desktop Server For Windows. The vulnerability grants a remote, unauthenticated attacker read access on the file system of the target via the web server.

**Name: Access:7**



[\*\*CVE-2022-25250\*\*](#) is a missing authentication for critical function vulnerability in the Axeda Agent and Axeda Desktop Server For Windows products. An attacker can leverage this vulnerability to remotely shut down a specific service on the target.

**Name: Access:7**



[\*\*CVE-2022-25251\*\*](#) is a missing authentication vulnerability in the Axeda Agent and Axeda Desktop Server For Windows products. This vulnerability can allow an attacker to send XML messages to a specific port without proper authentication, allowing the attacker to access and edit the program's configuration.

**Name: Access:7**



[\*\*CVE-2022-25252\*\*](#) is an improper check for unusual or exceptional conditions vulnerability in the Axeda Agent and Axeda Desktop Server For Windows products. This vulnerability can be leveraged by an unauthenticated attacker to crash the program.

**Name: Access:7**



# Pulse Secure



[CVE-2019-11510](#) is an unauthenticated arbitrary file disclosure vulnerability in Pulse Connect Secure SSL VPN, formerly known as Juniper SSL VPN. It received a CVSSv3 score of 10.0. It was featured as one of the top five vulnerabilities in the 2020 Threat Landscape Retrospective and has been exploited by several nation state and APT groups.



# RARLAB



[CVE-2022-30333](#) is a directory traversal vulnerability in the archive extraction tool known as UnRAR by RARLAB. An attacker could exploit this vulnerability against vulnerable Zimbra Collaboration Suite instances by sending a specially crafted email to a vulnerable target containing a malicious RAR attachment. No user interaction is required to exploit this flaw, because Zimbra will extract the malicious RAR file, which would be processed by the underlying UnRAR library.



# SAP



[CVE-2022-22532](#) is an HTTP request smuggling vulnerability in the SAP Internet Communication Manager (ICM). It does not require authentication or user interaction to exploit. In more complex scenarios, an attacker could leverage this flaw for RCE.

**Name: ICMAD**



[CVE-2022-22533](#) is a memory leak in the memory pipe management of the SAP ICM that could lead to DoS. An attacker could exploit this flaw using specially crafted HTTP(S) requests to consume all MPI resources.

**Name: ICMAD**



[CVE-2022-22536](#) is a memory pipe desynchronization vulnerability in the SAP ICM. An unauthenticated remote attacker could exploit the vulnerability using a simple HTTP request and achieve full system takeover.

**Name: ICMAD**



## SolarWinds



[CVE-2021-35247](#) is an improper input validation vulnerability in the Serv-U web login screen. It was exploited by attackers in January 2022 in order to propagate attacks using the Log4j vulnerabilities.



## SonicWall



[CVE-2021-20038](#) is an unauthenticated stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod\_cgi module environment variables that could lead to RCE as a 'nobody' user in the appliance.



[CVE-2022-22274](#) is a stack-based buffer overflow vulnerability in SonicOS. An unauthenticated, remote attacker could exploit this flaw to trigger a DoS and potentially achieve code execution in products like SonicWall Firewalls.



## Sophos



[CVE-2022-1040](#) is an authentication bypass vulnerability in the Sophos Firewall User Portal and Webadmin. Successful exploitation would result in RCE. Sophos reported that this vulnerability has been exploited in the wild.



[CVE-2022-3236](#) is a code injection vulnerability in the User Portal and Webadmin of the Sophos Firewall. An unauthenticated attacker could exploit this vulnerability by sending specially crafted requests to the User Portal or Webadmin of the Sophos Firewall that is externally accessible. Successful exploitation would allow for RCE.



## Trend Micro



[CVE-2022-26871](#) is an arbitrary file upload vulnerability in Trend Micro Apex Central (in both on-premises and as-a-service). Successful exploitation could grant an attacker RCE.



[CVE-2022-40139](#) is an improper validation vulnerability in the “rollback” functionality, which is used to revert Apex One agents to older versions. The vulnerability exists because Apex One agents are able to download unverified components, which could lead to code execution. While this vulnerability can only be exploited by an attacker with access to the Apex One administrative console, there have been reports of active exploitation.



## VMware



[CVE-2021-39144](#) is a RCE vulnerability in XStream, an open source library used for object serialization. This vulnerability was originally patched on August 22, 2021 in XStream version 1.4.18. VMware Cloud Foundation uses XStream for input serialization in its Network Security Virtualization for vSphere (NSX-V) solution. An attacker could exploit this vulnerability by targeting an unauthenticated endpoint in NSX-V to gain RCE privileges as root.



[CVE-2022-22948](#) is a local information disclosure vulnerability in vCenter Server. An authenticated, local attacker with low-privileged user access to a vulnerable vCenter Server could exploit this flaw to obtain sensitive information. This vulnerability is likely to be paired with other VMware vCenter Server bugs as part of an attack chain.



[CVE-2022-22954](#) is a server-side template injection vulnerability in the VMware Workspace ONE Access and Identity Manager. An unauthenticated attacker with network access could exploit this vulnerability by sending a specially crafted request to a vulnerable VMware Workspace ONE or Identity Manager.



[CVE-2022-22955](#) and [CVE-2022-22956](#) are authentication bypass vulnerabilities in the OAuth 2.0 Access Control Services (ACS) framework within VMware Workspace ONE. An unauthenticated attacker could send specially crafted requests to vulnerable and exposed OAuth2.0 endpoints in VMware Workspace ONE in order to successfully authenticate to the Workspace ONE instance.



[CVE-2022-22957](#) and [CVE-2022-22958](#) are authenticated RCE vulnerabilities in VMware Workspace ONE Access, Identity Manager and vRealize Automation. An attacker with administrative access can exploit these flaws by triggering the deserialization of untrusted data through malicious JDBC URI.



## VMware Continued >>

---

[CVE-2022-22963](#) is a RCE vulnerability in the routing functionality Spring Cloud Function. An attacker could exploit this flaw with a specially crafted HTTP request using the spring expression language.



[CVE-2022-22965](#) is a RCE vulnerability in the Spring Framework. It is a patch bypass of CVE-2010-1622. This vulnerability has several prerequisites for exploitation, including that applications must be running Java Development Kit version 9 or higher and use Apache Tomcat as the Servlet container.

**Name: Spring4Shell**



[CVE-2022-22972](#) and [CVE-2022-31656](#) are authentication bypass vulnerabilities in VMware Workspace ONE Access, Identity Manager and vRealize Automation that affects local domain users. In order to exploit this vulnerability, a remote attacker capable of accessing the respective user interface could bypass the authentication for these various products.



[CVE-2022-22973](#) is a local privilege escalation vulnerability in the VMware Workspace ONE Access and Identity Manager. In order to exploit this vulnerability, an attacker would need to have local access to the vulnerable instances of Workspace ONE Access and Identity Manager. Successful exploitation would allow an attacker to gain “root” privileges.



## WatchGuard

---



[CVE-2022-23176](#) is a privilege escalation vulnerability in WatchGuard Firebox and XTM appliances. When exploited, this vulnerability could allow an authenticated, yet unprivileged, remote attacker access with a privileged management session via exposed management access. This vulnerability was exploited by Russian threat actor Sandworm, according to CISA.



## WordPress Plugin

---



[CVE-2022-3180](#) is an unauthenticated privilege escalation vulnerability in the premium WordPress plugin called WP Gateway. An unauthenticated attacker could exploit this vulnerability to insert a malicious administrator onto a vulnerable WordPress site, enabling them to take over the site.





[\*\*CVE-2022-24682\*\*](#) is an XSS vulnerability in the Zimbra Calendar feature in Zimbra Collaboration Suite. An attacker could exploit this vulnerability by placing a specially crafted JavaScript HTML containing executable code inside of element attributes. This code would be injected into the document after being unescaped.



[\*\*CVE-2022-27924\*\*](#) is a memcache injection vulnerability in Zimbra Collaboration Suite. An unauthenticated attacker could steal login credentials by poisoning a vulnerable Zimbra Collaboration instance's IMAP route cache entries to gain unauthorized access to a company's email server.



[\*\*CVE-2022-27925\*\*](#) is an authentication bypass vulnerability in the Zimbra Collaboration MailboxImport Servlet. An authenticated attacker with administrative permissions could exploit the flaw by uploading files to the vulnerable system. Researchers discovered this flaw being leveraged as part of a vulnerability chain with CVE-2022-37042, a patch bypass of CVE-2022-27925. Combining the two flaws could allow an attacker to exploit this flaw as an unauthenticated attacker, resulting in RCE.



[\*\*CVE-2022-37042\*\*](#) is an authentication bypass vulnerability in the Zimbra MailboxImportServlet. An attacker could exploit this vulnerability by uploading arbitrary files to the system, which would be extracted using the mboximport functionality. Successful exploitation would result in path traversal and RCE.



[\*\*CVE-2022-41352\*\*](#) is an unpatched RCE vulnerability in Zimbra Collaboration Suite discovered in the wild due to active exploitation. The vulnerability is due to the method (cpio) in which Zimbra's antivirus engine (Amavis) scans inbound emails. This vulnerability, CVE-2022-41352 is effectively identical to CVE-2022-30333 but leverages a different file format. It is also a byproduct of a much older (unfixed) vulnerability, CVE-2015-1197.



## Zoho



[CVE-2021-40539](#) is a REST API authentication bypass vulnerability in ManageEngine ADSelfService Plus. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to a vulnerable host. Successful exploitation would grant an attacker RCE. CVE-2021-40539 has been exploited to deploy webshells and establish persistence in target environments.



[CVE-2021-44077](#) is an unauthenticated RCE vulnerability in ManageEngine ServiceDesk Plus caused by a security misconfiguration. It affects on-premises deployments up to version 11306.



[CVE-2022-35405](#) is an unauthenticated RCE vulnerability in Zoho ManageEngine Password Manager Pro and PAM360. Zoho ManageEngine Access Manager Plus is also affected, but requires an attacker to be authenticated.



## Zoom



[CVE-2022-28751](#) is a local privilege escalation vulnerability in the Zoom Client for Meetings on macOS. The vulnerability resides due to an issue in the update process due to a package signature validation issue. A local, authenticated attacker with low privileges could exploit the vulnerability to elevate to root privileges.



[CVE-2022-28756](#) is a local privilege escalation vulnerability in the Zoom Client for Meetings on macOS. The vulnerability resides in the auto-update process of the Zoom Client. A local, authenticated attacker with low privileges could exploit the vulnerability to elevate to root privileges. The fix for this vulnerability addresses CVE-2022-28751.



[CVE-2022-28762](#) is a misconfigured debugging port in Zoom Apps in the Zoom Client for Meetings for macOS. A local attacker could exploit this vulnerability by connecting to the debugging port and control the Zoom apps running in the Zoom client.





6100 Merriweather Drive

12th Floor

Columbia, MD 21044

North America: +1(410) 872-0555

Latin America: +1(443) 545-2278

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