2023 QUALYS TRURISK RESEARCH REPORT

On the State of Vulnerabilities, Top Exploits, and Five Risk Facts Learned from Threat Analytics for Improving Security Posture from 2022 Data

Qualys Threat Research Unit

TABLE OF CONTENTS

FOREWORD

The explosion of digital transformation in every business today is inevitable. Companies are increasingly competing by enhancing their customers' digital experience. Similarly, global government organizations are significantly accelerating digital programs enabling citizens with e-governance, biometric identities and cardless payments to overcome financial exclusion. This has led to staggering amounts of software being developed in the last few years and a surge in software vulnerabilities with many more to come. Combine this with the shortage of skilled cybersecurity professionals, and CISOs and security teams are left with the daunting challenge of keeping up with the sheer volume of information coming at them. CISOs and security teams must continuously work to keep up with the fast pace of technological advancement and evolving cyber threats to reach their goal of reducing their organization's risk.

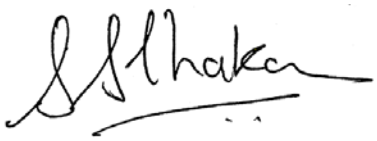
Today's cybersecurity tools, which solely focus on generating more and more detections and alerts are not enough to help secure organizations. Organizations require assistance in prioritizing the most severe vulnerabilities present in their critical assets and resolving them before attackers exploit them. Additionally, they need a risk-based approach to quantify and align cyber risk to their business and communicate effectively with their executives and boards.

Qualys' passion and vision for helping companies minimize cyber risks has driven us to innovate by launching VMDR with TruRisk and patch management on our platform. Over the past 20+ years, we have operated a vast cloud platform that conducted 6+ billion scans, managed 90+ million agents, and deployed 45+ million patches in 2022 alone. This large pool of anonymized, real-time data allows us the opportunity to provide insights that assist organizations in enhancing their security programs.

Our research team took a deep dive into our platform and its 13+ trillion anonymized data points to determine which vulnerabilities cause the highest risk to organizations. This data, overlayed with threat intelligence and original research conducted by The Qualys Threat Research Unit (TRU), exposes the intricacies of threat actor activities and operations. With vulnerability management, patching and endpoint detection and response (EDR) on a single platform, our TRU researchers get valuable insights into how threat actors behave pre and post-exploitation.

Defining risk is more important than ever in setting a cybersecurity strategy. Today's security teams must think holistically about attack paths, examine threat actor behaviors to understand what could wreak the most havoc, and quickly control threat activity when a breach occurs.

We encourage everyone – from practitioners to CISOs – to leverage the data and insights in this report to support their security initiatives and help facilitate more profound conversations with executives and board members that will enhance security posture. The report offers a reliable resource for security practitioners seeking data-driven, real-world, and actionable perspectives on vulnerabilities and trends critical to organizations across all industries and sizes. We hope that these insights will assist your teams in overcoming those seeking to harm your digital infrastructure.



Sumedh Thakar
President and CEO, Qualys

INTRODUCTION

Many cybersecurity companies today focus solely on detection, which is a large part of the overall equation. But detection alone is not enough to reduce and eliminate risks within your environment. Stakeholders must also discover and remediate the risks that threaten a company or forever play a game of catch-up with threat actors.

You can brush your teeth and floss every day, or you can risk cavities, or worse, and hope a dentist can fix larger problems later. Using detection tools alone provides a diagnostic, confirming a cavity — but still requires the painful path of extracting the infection. A wise approach is to focus first on finding flaws and reducing risk. This strategy requires understanding how vulnerabilities and misconfigurations are commonly leveraged and how to reduce the mean time to remediation (MTTR). Which do you prefer: brushing your teeth or being numbed by Novocain?

No matter the difference in size, geography or industry, a CISO's number one job is to manage cyber risk. Qualys helps organizations understand their risk exposure by providing comprehensive information on their unique environments and associated risks — which, left unattended, could upend their operations. Adversaries make it their business to understand the vulnerabilities and weaknesses within their victims' environments, which can shift the balance of power and control in their favor, enabling cybercriminals to exploit vulnerabilities that organizations may not be aware of. In this report, the Qualys Threat Research Unit (TRU) investigates the primary techniques explored by adversaries to exploit vulnerabilities, compromise systems and infiltrate organizations.

TRU works to secure and defend the digital world from threat actors who seed chaos and erode trust in business operations. From building vulnerability signatures, to writing detection rules, researching and finding zero-day threats, finding and reversing custom malware, reducing attack surface exposure and other advanced threat research activities — TRU works day and night to protect our customers' cyber assets.

I hope this report offers you the same opportunity and direction that it offers me: to increase awareness of what attackers are adding to their Swiss Army knife of tools so you can create swift countermeasures. Above all, I want to inspire defenders by showing that their work does make a difference!

Travis Smith
Vice President, Threat Research Unit, Qualys

Key Findings

In 2022, Qualys detected more than 2.3 billion vulnerabilities around the globe. By mining anonymous detection statistics from our global platform, TRU discovered unique insights into the vulnerabilities found on many devices, security of web applications, misconfiguration of on-premises devices, and cloud security posture. These data points reveal Risk Facts that universally apply across industries and organizations:

1. **Speed is the key to out-maneuvering adversaries**
2. **Automation is the difference between success and failure**
3. **Initial Access Brokers (IABs) attack what organizations ignore**
4. **Misconfigurations still prevalent in web applications**
5. **Infrastructure misconfigurations open the door to ransomware**

Methodology

1. This report focuses on 163 unique Common Vulnerabilities and Exposures (CVEs) announced in 2022, capable of introducing the highest level of risk to organizations across industries and all sizes.
2. Anonymous detection statistics for the 163 CVEs were analyzed to establish their impact on enterprise security and the potential for breaches.
3. Anonymous Web Application Security (WAS) data was examined, and detections were mapped to the OWASP Top 10 application security risks.
4. Anonymous detections from Policy Compliance (PC) scans related to endpoint scans using Center for Internet Security (CIS), Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGs), and Qualys Ransomware Protection policies to analyze commonly failing controls.
5. Discovery of the most common failing controls was enabled by analysis of anonymous scan detections from CIS Hardening Benchmarks for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

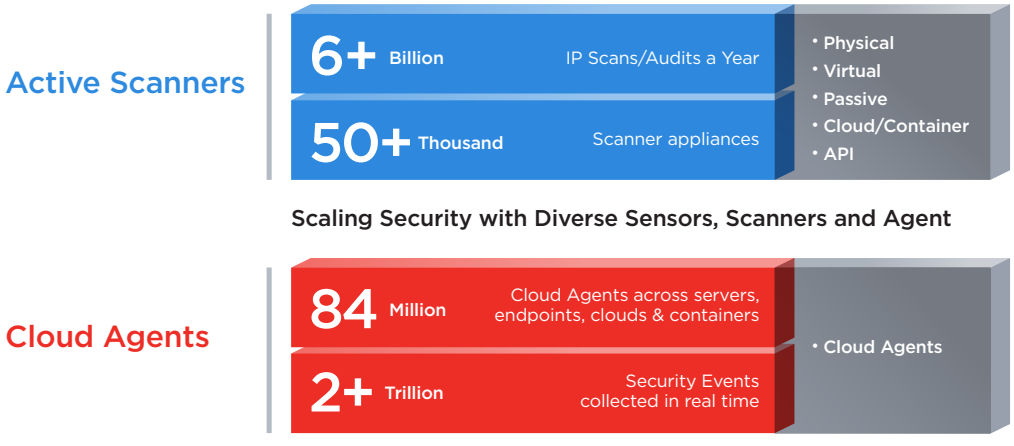


Figure 1: Qualys Platform — Deploying Anywhere

STATE OF VULNERABILITIES

The total number of reported vulnerabilities has exploded in recent years. The 1990s clocked 2,594 vulnerabilities in total, which rose 796% to 37,231 in the 2000s; since 2010 another 135,284 were discovered. A cumulative growth rate in vulnerabilities of 5,116% over this period seems startling. The trend continued during 2022 when more than 25,000 vulnerabilities received a unique CVE.

Given the wide assortment of classifications and Common Vulnerability Scoring System (CVSS) scores, not all 25,000 are created equal. Some are more dangerous than others based on their malicious usage by threat actors or patch difficulty — and many are still unprioritized.

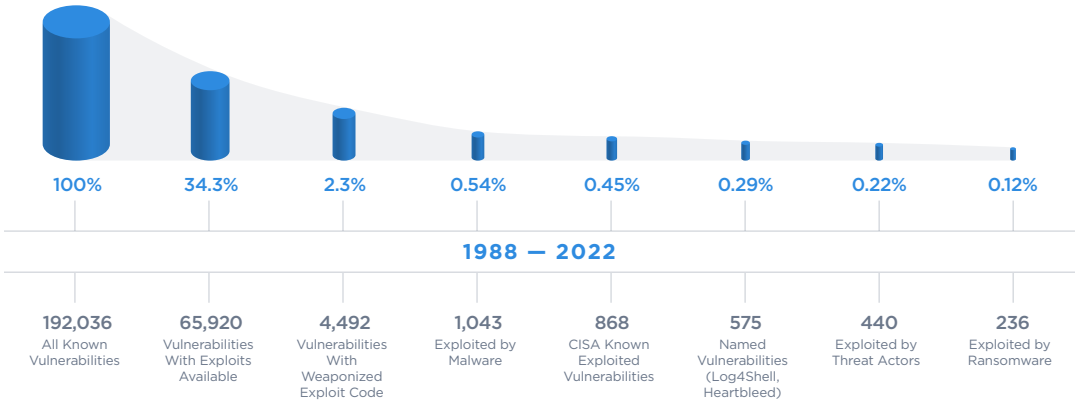


Figure 2: Evolution of vulnerability threat landscape, 1988 – 2022

Within the universe of more than 192,000 known vulnerabilities, only a subset of those introduce the most risk to the organization. While the absolute number of vulnerabilities causing risk might be small, it is a dynamically evolving subset with older vulnerabilities getting new exploits regularly. This makes it important to continuously monitor threat intelligence and focusing on vulnerabilities that cause risk at any given point of time. By assessing cyber risk in terms of business risk, individual organizations can put these astronomical numbers into perspective. This report describes which are the most dangerous, categorizing them into one or more of the following:

Exploit Available	A weaponized exploit available publicly
Threat Actor	Exploited by and associated with a named threat actor
Malware	One or more pieces of malware known to exploit the vulnerability
Ransomware	Ransomware known to exploit the vulnerability
CISA KEV	Was added to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog
Named Vulnerability	Name was given to the vulnerability by security industry or media

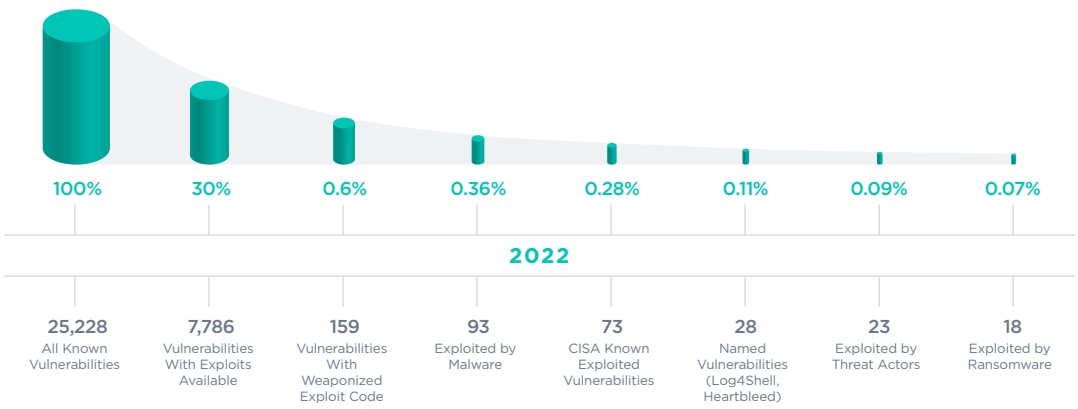


Figure 3: Evolution of vulnerability threat landscape in 2022

During 2022, the proportion of weaponized vulnerabilities among all published vulnerabilities decreased. Nonetheless, numerous vulnerabilities from previous years were utilized for the first time by threat actors or malware, resulting in weaponization. Throughout the year, a total of 539 such vulnerabilities from previous years were exploited in some capacity. Of the 539 newly weaponized vulnerabilities, 118 were older than three years and were as old as CVE-2004-0210 which was published in August 2004.

	CISA KEV	WEAPONIZED	THREAT ACTOR	RANSOMWARE
Vulnerability Count	453	237	62	50

Figure 4: Vulnerabilities published prior to 2022 which are now being exploited in 2022

What this shows is that threat actors are not only adopting new vulnerabilities which are new and novel, they are also looking at exploiting vulnerabilities which remain unpatched within the organizations they encounter. This highlights that organizations need to take into account the threat landscape to fully understand how to prioritize vulnerabilities to address in their environments.

TOP EXPLOITS IN 2022

The criteria to define which vulnerabilities were the most exploited during calendar year 2022 was simple: those which wreaked the most havoc. These vulnerabilities fall under the six categories mentioned above, which are presented in Table 1 and followed by individual descriptions.

CVE	QVS	CISA KEV	THREAT ACTOR (COUNT)	RANSOM-WARE	MALWARE (COUNT)	MTTR (DAYS)	PATCH RATE
CVE-2022-30190	100	Y	4	Y	6	28.4	91.21%
CVE-2022-26134	100	Y	1	Y	4	28.5	58.30%
CVE-2022-22954	100	Y	1	Y	2	14.3	87.38%
CVE-2022-1040	100	Y	3	Y	1	70.0	34.70%
CVE-2022-24521	95	Y	2	Y	4	20.6	90.00%

Table 1: Top Exploited Vulnerabilities in 2022

CVE-2022-30190
Follina

This vulnerability poses a significant threat to organizations because an attacker can execute arbitrary code via various applications such as Microsoft Word. The exploit leverages the built-in Microsoft URL handlers to trigger the msdt.exe process, which can then be used to run PowerShell commands. This allows Remote Code Execution (RCE), which can provide the ability to install programs, access/modify data, or create new user accounts.

This vulnerability has been leveraged by at least 4 named threat actors and multiple malware families. The notorious Fancy Bear and Wizard Spider groups are known to exploit this CVE, as are the lesser known Luckycat and UAC-0098 groups. Some of the more well-known ransomware families to leverage this vulnerability are Qakbot, Skeeyah, and Black Basta. While the U.S. National Institute of Standards and Technology's National Vulnerability Database (NVD) published the Follina CVE on June 1, 2022, and was known to be weaponized in less than a day, CISA did not add it to the KEV Catalog until 13 days following its disclosure on that month's Microsoft Patch Tuesday. During 2022, this CVE was detected 12.8 million times around the world and patched on average in 28.1 days, reaching an effective patch rate of 91.21%.

CVE-2022-26134
Atlassian Confluence Remote Code Execution Vulnerability

This critical severity vulnerability allows unauthenticated remote code execution. As an Object-Graph Navigation Language (OGNL) injection vulnerability, it allows an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The CVE can be exploited by sending a specially crafted Hypertext Transfer Protocol (HTTP) request containing an OGNL expression in the Uniform Resource Identifier (URI) to the target server, which results in remote code execution. This CVE was an active vulnerability in all Confluence Servers and Data Center versions prior to distribution of a patched version.

This vulnerability was exploited by the Sparkling Goblin threat actors' group, while also known to be leveraged by two ransomware families — particularly the Cerber and AvosLocker variants. While this CVE was detected only about 3,000 times, it poses significant risk due to the information it stores, its exposure to the internet, and its ease of exploitation. This vulnerability was added to the CISA KEV before being published by the NVD. This vulnerability is the second slowest (behind the Sophos Firewall Authentication Bypass [CVE-2022-1040] vulnerability) for remediations, being patched in 28.5 days with a 58.3% patch efficacy.

CVE-2022-22954
VMware Workspace ONE Server-Side Template Injection Vulnerability

This CVE is a remote code execution vulnerability arising from a server-side template injection in the VMware Workspace ONE Access and Identity Manager. The vulnerability can be easily exploited with a specially crafted HTTP request and poses a significant risk because anyone with network access to a vulnerable instance can initiate this exploit to execute arbitrary code on the system.

Multiple vulnerabilities were discovered in VMware Workspace ONE in 2022 — five were weaponized and two were added to the CISA KEV list, yet only one was leveraged by threat actors and ransomware groups. This vulnerability was weaponized in less than a day and added to the CISA KEV list within just three days following its disclosure. Only the Rocket Kitten group is known to be exploiting this vulnerability in the wild. However multiple malware and ransomware families do leverage this, particularly the RAR1Ransom and Clop families. Patching has been faster for this vulnerability, within 14.3 days for an 87.3% patch efficacy.

CVE-2022-1040
Sophos Firewall Authentication Bypass

CVE-2022-1040 is an authentication bypass vulnerability in the user portal and web admin of the Sophos Firewall running version v18.4 MR3 or older. Successful exploitation allows an attacker to bypass authentication and gain unauthorized access to the firewall to execute arbitrary code.

This vulnerability is leveraged by two threat actors, LuckyCat and DriftingCloud, and is leveraged by the Ragnarok ransomware family. Considering the target is a firewall device allowing direct connection to the internet, this CVE poses a serious issue that requires urgent remediation. It was added to CISA KEV six days after its publication to the NVD. Qualys found more than 6,000 vulnerable instances resolved on average in 70 days with a 34.7% patch efficacy.

CVE-2022-24521

Windows CLFS Driver Privilege Escalation Vulnerability

This CVE affects the Windows Common Log File System (CLFS) driver for Microsoft Windows. Successful exploitation allows for privilege escalation and is likely to be used in tandem with additional exploit techniques for gaining code execution abilities. It results in an Elevation of Privilege (EoP) in the Windows Common Log File System (CLFS) driver. Vulnerabilities like this CVE are typically leveraged after an attacker has already gained access to the vulnerable system. The attacker will then use the EoP vulnerability to gain higher permissions such as administrator-level access. CVE-2022-24521 was reported to Microsoft by the National Security Agency (NSA). It was detected in more than 14 million instances and added to the CISA KEV two days before NVD published the CVE. Two threat actors, UNC2596 and Vice Society, have been known to leverage this vulnerability. Other exploits were by four malware families, including four ransomware families: N13V/RedAlert, Cuba, and Yunluowang. Organizations patched this vulnerability within 20.6 days at a 90% patch efficacy during 2022.

FIVE RISK FACTS LEARNED FROM THREAT ANALYTICS IN 2022

RISK FACT 1

1 SPEED IS THE KEY TO OUT-MANEUVERING ADVERSARIES

The doubling of disclosed vulnerabilities over the last five years, the speed at which vulnerabilities are weaponized, and the cyber talent shortage have left teams struggling to wade through a mountain of vulnerabilities with no way to fix them all. Security teams need a systematic approach to cut through the noise and prioritize fixing the most critical vulnerabilities that will reduce risk and enable them to keep up with threat actors.

On average, weaponized vulnerabilities are patched within 30.6 days while only being patched an average of 57.7% of the time. These same vulnerabilities are weaponized by attackers in 19.5 days on average. This means that attackers have 11.1 days of exploitation opportunities before organizations begin patching. Arguably the remediation activity accelerates after weaponization happens. Hence, it is very important to predict which vulnerabilities could be weaponized and patch them as early as possible so an emergency drill can be avoided.

A defender's mean time to remediation (MTTR) shows a slight change in how organizations respond to urgent threats. Vulnerabilities known to be leveraged by named threat actors were remediated eight days faster than those without association to known threat actors. But while defenders are quick to address these, attackers are also quick to weaponize. Threat actors were faster to leverage vulnerabilities that are known to be exploited or were cataloged on CISA's Known Exploited Vulnerabilities list when compared to those leveraged by malware and ransomware.

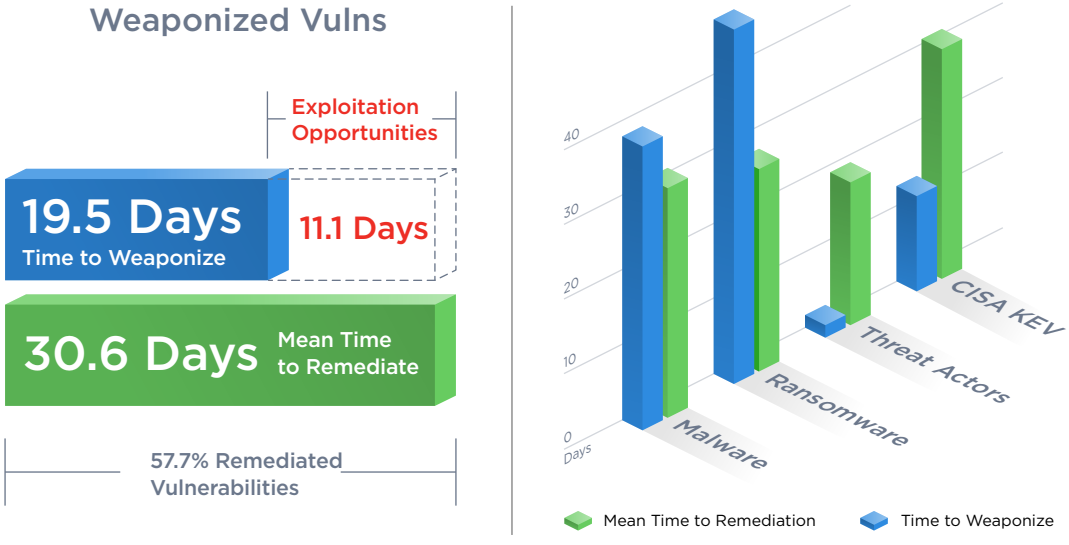


Figure 5: Time to Weaponize vs. MTTR for Vulnerabilities in 2022

Attribution of a vulnerability to a named threat actor is a time-consuming and extremely difficult process. On average, attribution happens 95 days (about three months) after a vulnerability is published and 74.3 days (about two and a half months) after the CVE is patched. Data suggests that when a vulnerability is associated with a named threat actor, it does not necessarily lead to faster patching due to various factors. Organizations often need more resources for their cybersecurity teams, which means they prioritize patching based on criticality and active exploitation, not necessarily on threat actor association. Patch management can be complex, involving compatibility testing, scheduling downtime, and coordinating with multiple teams, causing delays in patch deployment. Accurate attribution of a cyberattack to a specific threat actor is complex, and uncertainty in attribution can affect patch prioritization. Additionally, organizations might underestimate the risk associated with a vulnerability if they believe the named threat actor is not targeting their industry or region, which may result in slower patch deployment. Finally, patches for specific vulnerabilities may not be immediately available from the vendor, causing delays in patching even when organizations are aware of the risk.

The analysis found that Microsoft Windows and Google Chrome represented every spot in the top 10 most detected CVEs in 2022, as shown in Table 2. This makes sense since Windows and Chrome are at the top in terms of market share for operating systems and browsers, respectively.

CVE	TITLE	DETECTIONS (MILLION)	MTTR (DAYS)
CVE-2022-2856	Google Chrome Intents Insufficient Input Validation Vulnerability	22.4	11.5
CVE-2022-41049	Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability	17.1	10.3
CVE-2022-4135	Google Chromium Heap Buffer Overflow Vulnerability	17.0	2.03
CVE-2022-2294	WebRTC Heap Buffer Overflow Vulnerability	16.5	13.8
CVE-2022-3075	Google Chromium Insufficient Data Validation Vulnerability	16.1	9.8
CVE-2022-30170	Windows Credential Roaming Service Elevation of Privilege Vulnerability	15.4	13.2
CVE-2022-24521	Microsoft Windows Common Log File System CLFS Driver Privilege Escalation Vulnerability	14.0	20.5
CVE-2022-26904	Microsoft Windows User Profile Service Privilege Escalation Vulnerability	13.9	10.8
CVE-2022-37969	Microsoft Windows CLFS Driver Privilege Escalation Vulnerability	13.7	10.8
CVE-2022-1096	Google Chromium V8 Type Confusion Vulnerability	13.3	21.0

Table 2: Top 10 Vulnerabilities in 2022 Affecting Windows or Chrome

Visualizing the vulnerability data in scatter charts shows the full story. Figure 6 compares the age (X-axis) of a vulnerability to the percentage remediated (Y-axis) — a vivid picture of how organizations tackle these issues. The speed of remediation in Figure 6 varied wildly across all vulnerabilities.

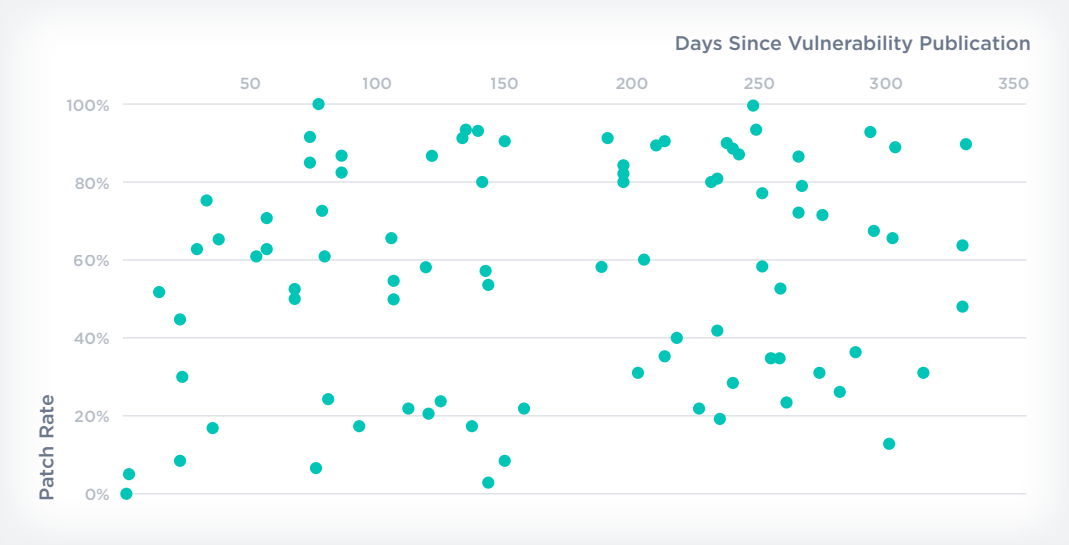


Figure 6: Comparing Weaponized Vulnerabilities in 2022 by Age vs. Percentage Remediated

Filtering the scatter chart to represent the top detections — Windows and Chrome — shows a definitive trendline of how organizations prioritize patching for the quickest result. As shown in Figure 7, results leveled out around a 90% patch rate, which suggests that the patches are deployed to approximately 90% of the organization's infrastructure before the next wave of monthly patching begins.

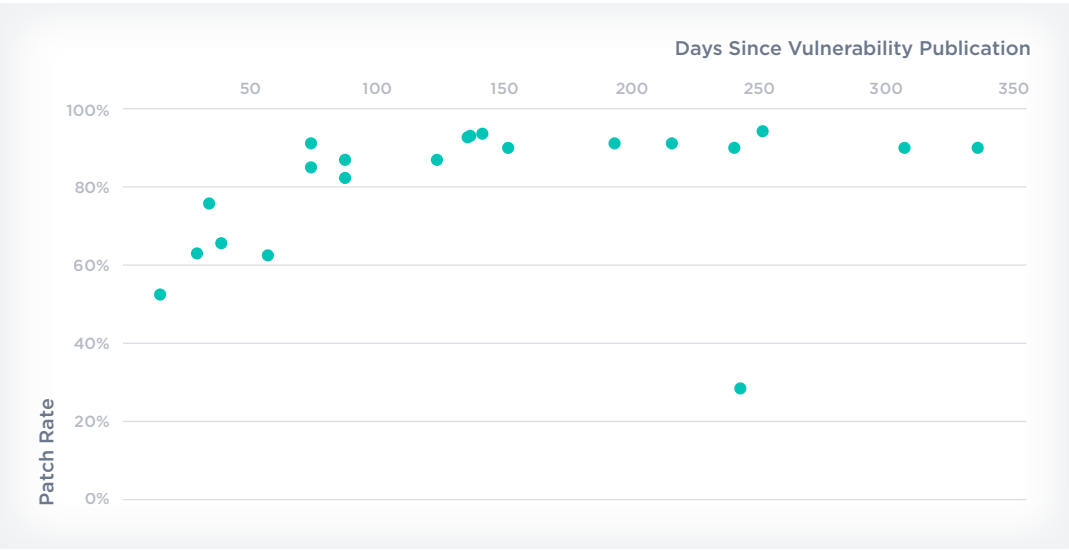


Figure 7: Comparing Weaponized Chrome/Windows Vulnerabilities in 2022 by Age vs. Percentage Remediated

The higher patch rate for weaponized Chrome/Windows vulnerabilities stems from two reasons. First, the number of critical vulnerabilities these two products receive are significantly higher than others, and organizations are quick to prioritize critical vulnerabilities that have the potential to pose the most risk. Second, both Windows and Chrome patches are easily automated — critical for allowing defenders the opportunity to catch up to the speed at which threat actors operate.

However, removing Windows and Chrome shows a much different story (Fig. 8) with no clear patterns in remediation prioritization for the remaining vulnerabilities. The extreme variations can be attributed to factors such as an inability to automate patching (representative of patching niche software, which is often more difficult), or security teams deciding that patching the vulnerability is of little importance unless it is moved to CISA's KEV list.

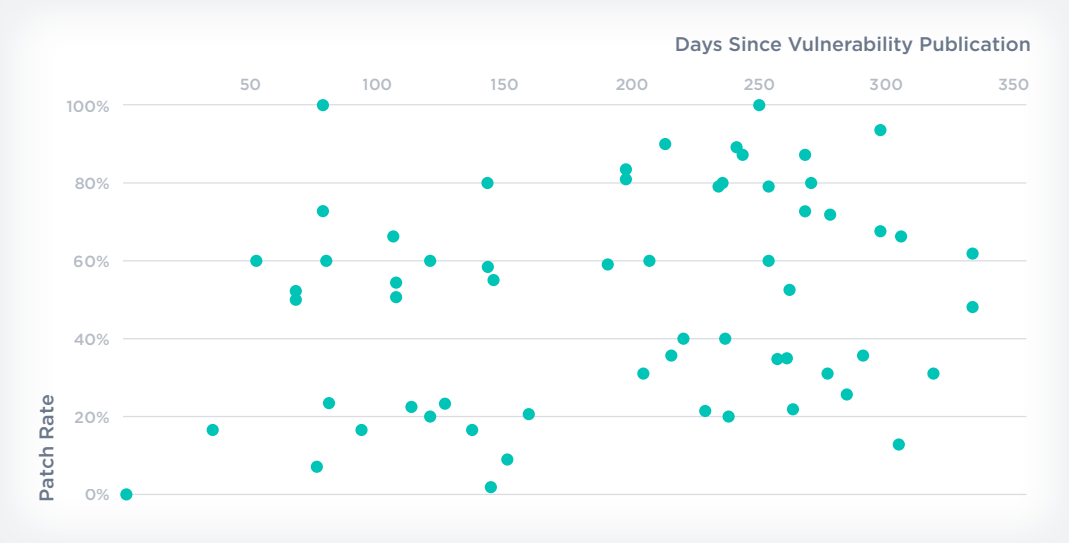


Figure 8: Comparing Weaponized Non-Chrome/Windows Vulnerabilities in 2022 by Age vs. Percentage Remediated

RISK FACT 2

2 AUTOMATION IS THE DIFFERENCE BETWEEN SUCCESS AND FAILURE

Automation across security infrastructure has become a necessity for every cyber arsenal. It allows organizations to eliminate manual and tedious tasks, which ultimately reduces the time and effort it takes to remediate vulnerabilities and frees up security staff to address more pressing concerns. Qualys Patch Management customers deployed more than 45 million patches, highlighting the shift in organizations migrating to more automated means to combat threat actors.

Most weaponized vulnerabilities discussed in the body of this study were in Chrome or Windows, due to the high prevalence of that browser and operating system. The mean time to remediation for these products globally is 17.4 days (about 2 and a half weeks) with an effective patch rate of 82.9%. Windows and Chrome are patched twice as fast and twice as often as other applications.

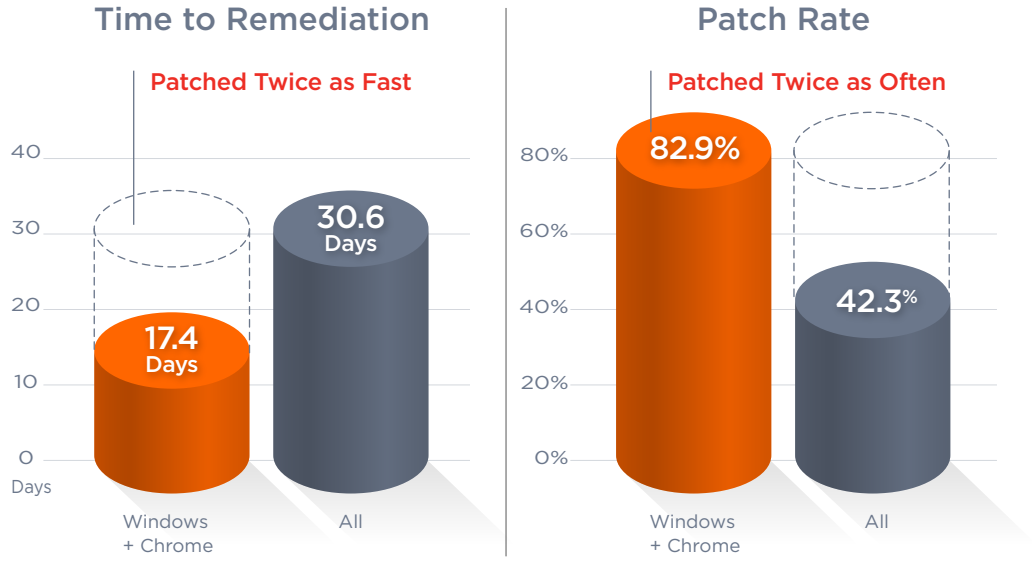


Figure 9: MTTR vs. Patch Rate for Chrome in Windows Vulnerabilities in 2022

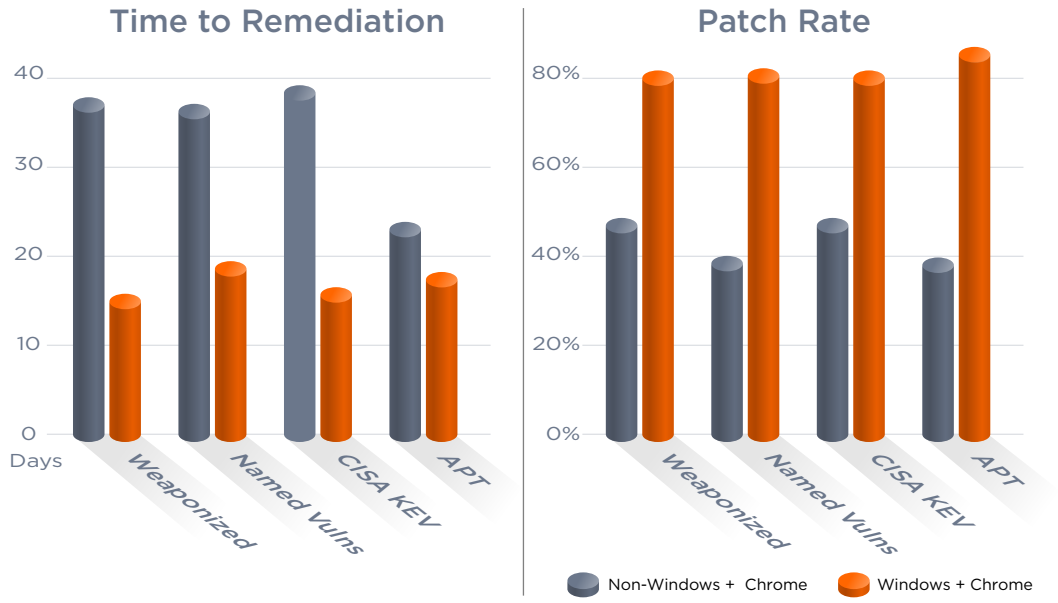


Figure 10: MTTR vs. Patch Rate for Chrome in Windows Vulnerabilities in 2022

Chrome and Windows comprise one-third of the weaponized vulnerabilities dataset, with 75% of these leveraged by named threat actors. Knowing these are prime risk vectors, organizations typically patch them first and most thoroughly.

The study reveals patches that are known to have the opportunity to be deployed automatically were deployed 45% more often and 36% faster than those of a manual nature. Vulnerabilities that were automatable with a patch management solution have a mean time to remediation of 25.5 days; where manually patched vulnerabilities were remediated in 39.8 days. The patch rate for the automatable set was 72.5% compared to 49.8% for those in the manual set. The extreme variations can be attributed to factors such as an inability to automate patching.

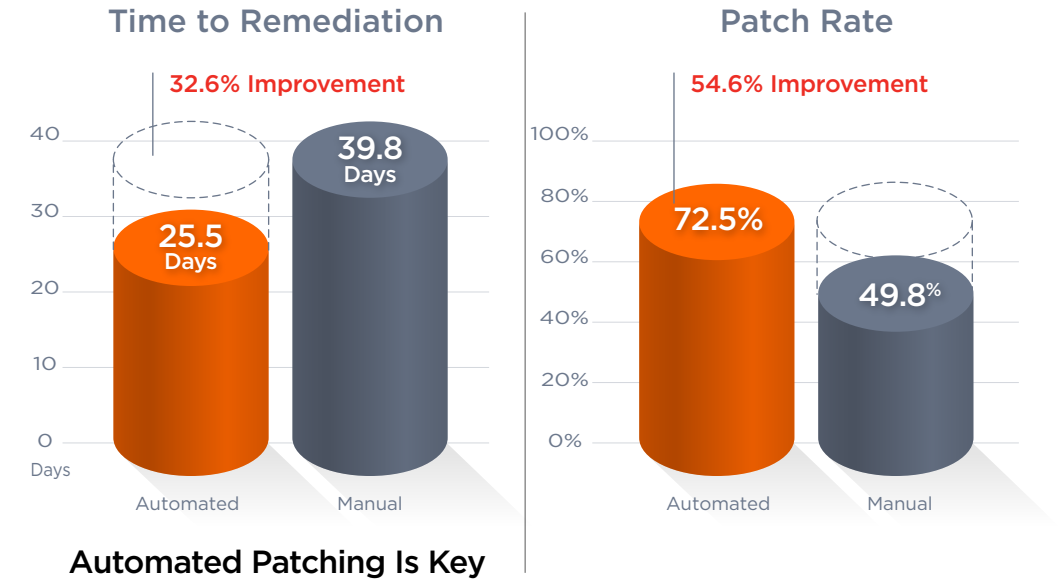


Figure 11: Automated Patching Improves MTTR for Vulnerabilities in 2022

RISK FACT 3

3 INITIAL ACCESS BROKERS ATTACK WHAT ORGANIZATIONS IGNORE

A growing trend in the threat actor landscape is a category called Initial Access Brokers (IABs), sometimes called "affiliates." TRU research shows the initial access point for IABs will follow one of multiple paths. In Figure 12, the top lane is where IABs seek to exploit the perimeter devices of their intended target, such as firewalls and web applications. IABs seek misconfigurations such as default passwords or exposed services to find a way in or exploit vulnerabilities for unpatched systems. Another path is leveraging valid credentials and gaining direct access to the environment. IABs will either attempt to steal the credentials, buy them in the dark web, which were stolen from other breaches, or guess/brute force the passwords. By leveraging valid accounts, the threat actor can move around the environment with more stealth than relying on exploitation.

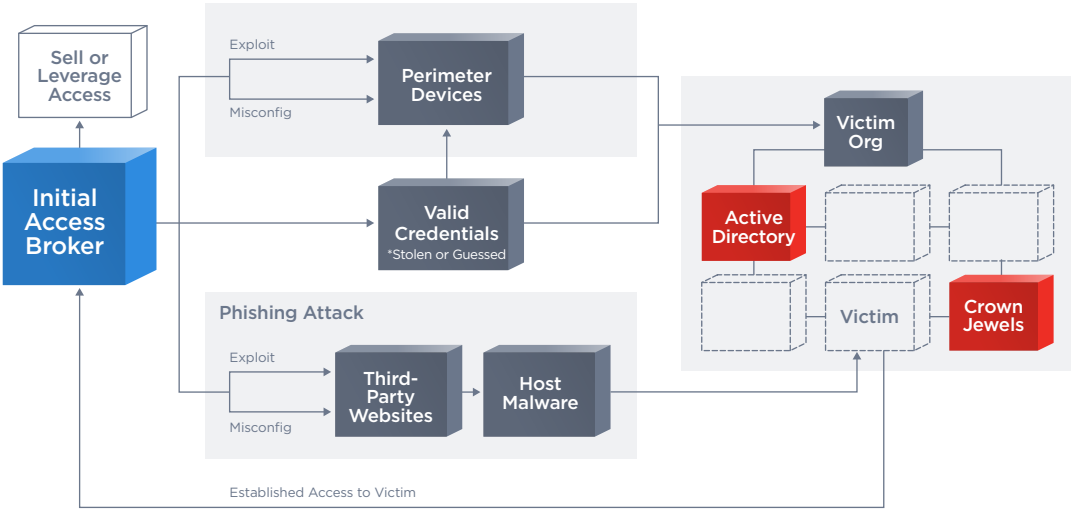


Figure 12: Attack Paths Used by Initial Access Brokers (IABs)

Finally, there are phishing attacks. IABs do not always stand up their own infrastructure to deploy requisite tooling. Instead, they breach trusted organizations just as they would attack perimeter devices of an intended victim. This beachhead allows the IAB attacker to upload malware — and deliver it via phishing to the intended target. Access then allows hunting for valuable data, such as access to Active Directory or finding the target company's crown jewels.

Acquisition of this information is then sold to another criminal gang or used by the attacker themselves. The motive is to deliver and profit from ransomware. During 2022, there were 17 new CVEs added to the IAB toolkit (see Table 3).

CVE	TITLE
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability
CVE-2022-22963	VMware Tanzu Spring Cloud Function Remote Code Execution Vulnerability
CVE-2022-22965	Spring Framework JDK 9+ Remote Code Execution Vulnerability
CVE-2022-24663	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets
CVE-2022-24664	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets
CVE-2022-24665	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability
CVE-2022-26706	A sandboxed process may be able to circumvent sandbox restriction in tvOS, iOS, iPadOS, watchOS, macOS Big Sur, and macOS Monterey
CVE-2022-26258	D-Link DIR-820L Remote Code Execution Vulnerability
CVE-2022-28958	D-Link DIR-816L Remote Code Execution Vulnerability
CVE-2022-31625	PHP RCE When Using Postgres Database Extension
CVE-2022-31626	PHP RCE When Using pdo_mysql Extension with mysqlnd Driver
CVE-2022-40684	Fortinet Multiple Products Authentication Bypass Vulnerability
CVE-2022-41040	Microsoft Exchange Server Server-Side Request Forgery Vulnerability
CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2022-41343	registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion
CVE-2022-41352	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability

Table 3: New Exploits Using Initial Access Brokers (IABs) During 2022

None of the vulnerabilities in Table 3 are related to Windows or Chrome. Many of these affect perimeter devices or applications encountered when an IAB attacker attempts initial access. Remediation timelines for these CVEs are much worse than for Windows and Chrome. IAB vulnerabilities have a mean time to remediation of 45.5 days, compared to 17.4 days for Windows and Chrome. The patch rates are also lower, patched at a rate of 68.3% compared to 82.9% for Windows and Chrome.

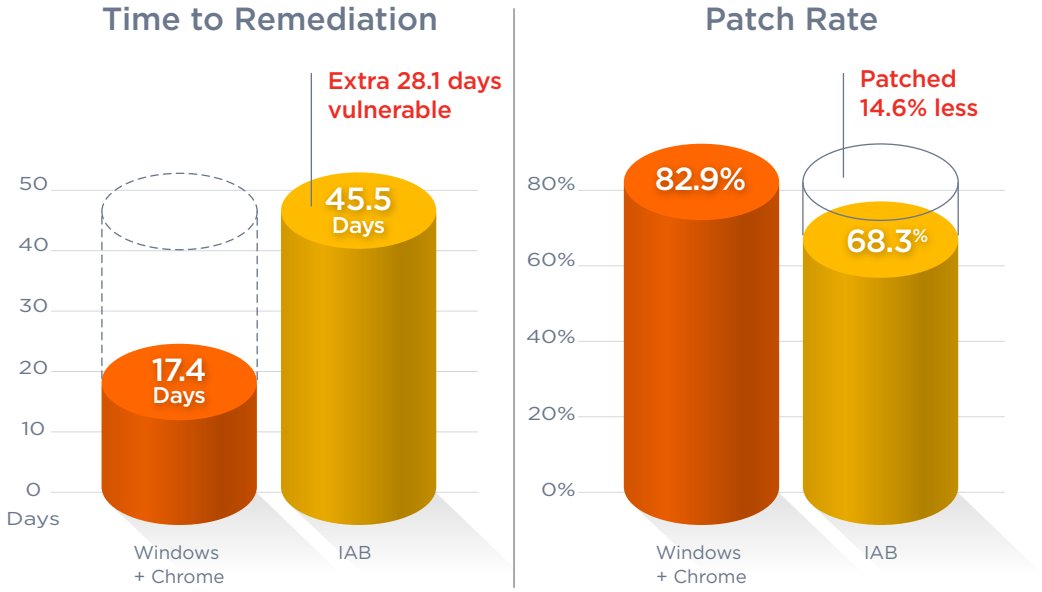


Figure 13: Remediation rates of Windows + Chrome

This data shows that because organizations are getting quicker at patching Windows and Chrome, threat actors — especially IABs — are forced to leverage vulnerabilities outside of the "big two." The data also suggests that when defenders control the narrative, threat actors are forced to switch their tactics, techniques, and procedures to more challenging attack paths. When this happens, threat actors tend to make more mistakes, create more noise, and generate more detection opportunities for defenders.

RISK FACT 4

4 MISCONFIGURATIONS STILL PREVALENT IN WEB APPLICATIONS

The Open Web Application Security Project (OWASP) Top 10 is a list of the most common and most critical vulnerabilities that can impact a web application. Security experts rely on the OWASP Top 10 when talking about web app security. The list helps developers prioritize and understand what to fix to make their applications more secure. Remarkably, while the Top 10's vulnerabilities incur minor repositioning from year to year, most have maintained a persistent presence since the Top 10 was first published in 2003!

This study included anonymized detections in 2022 from the Qualys Web Application Scanner, which globally scanned 370,000 web applications and correlated data against the OWASP Top 10. The scans revealed more than 25 million vulnerabilities, 33% of which were classified as OWASP Category A05: Misconfiguration. These misconfiguration vulnerabilities provided malicious actors with the capability to spread malware in about 24,000 web applications.

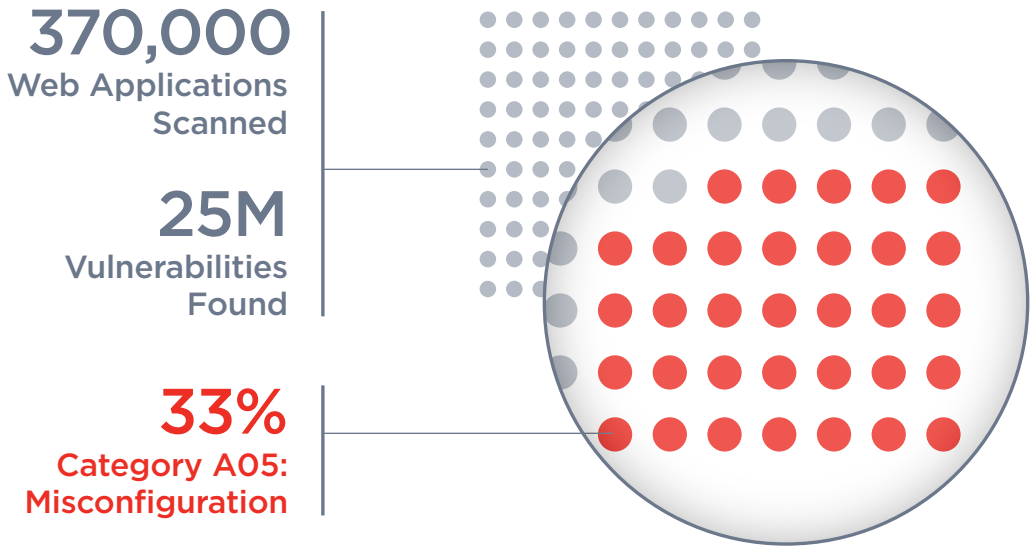


Figure 14: OWASP Top Vulnerability Discovered in 2022 by Web Application Scanning

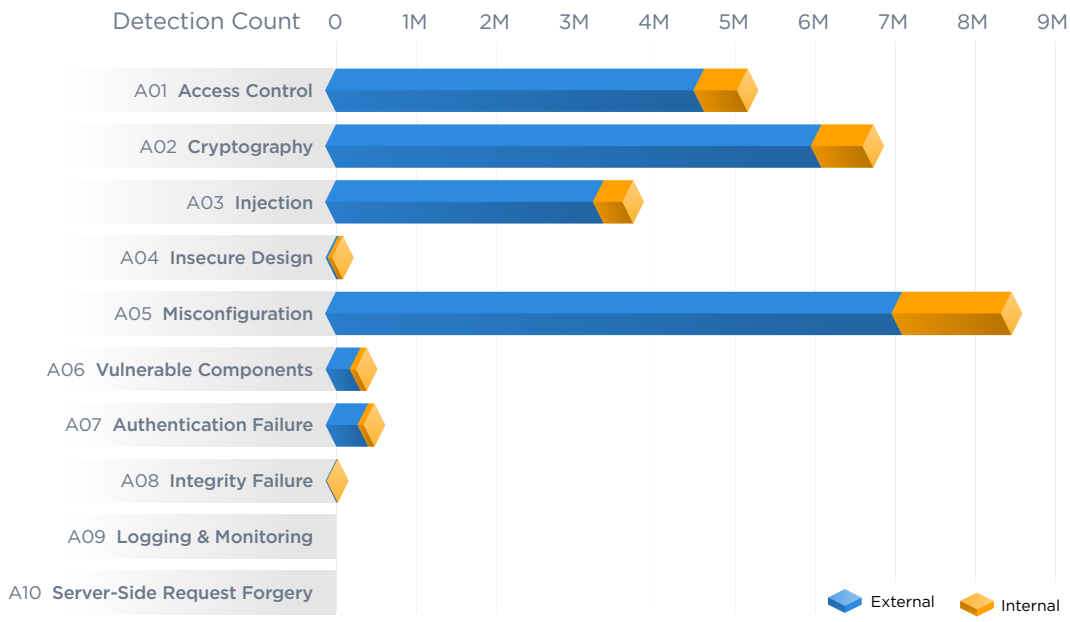


Figure 15: OWASP Top 10 Vulnerabilities Discovered in 2022 by Web Application Scanning

Misconfigurations largely entail improper controls used to protect web applications. Oftentimes this occurs when security best practices are not followed, such as not changing default permissions or passwords. Another type of misconfiguration can be applications that share too much information, such as detailed stack traces for errors. By not following security best practices, these web applications are vulnerable to a variety of attacks. For example, sophisticated attackers may use information disclosed in a verbose stack trace to identify web application technologies and mount a more advanced attack to breach a site. Even a simple error, such as not disabling directory listings, can trigger long-term issues if personally identifiable information (PII) is inadvertently exposed through misconfigurations.

The other top-detected categories are A02: Cryptographic Failures, A01: Broken Access Control, and A03: Injection. Cryptographic Failures can expose sensitive data by weak cryptographic controls (or worse, no cryptography). Misconfigurations enabling these attacks can cause session hijacking, stolen user credentials, and attacks against other data at rest or in transit.

Broken Access Control errors leverage violations of permission rights to gain access to web applications or resources. Examples include forced browsing to pages behind authentication or unauthorized privilege escalation for authenticated users. In some cases, access control is completely missing, such as the Optus data breach, where malicious actors discovered an unprotected API endpoint that allowed access to over 10 million customer records.

Finally, the injection category is the culprit of many common web application attacks, such as SQL and command injection attacks, Cross-Site Scripting (XSS), and Cross-Site Request Forgeries (CSRF). Many of these attack techniques have existed since the first web applications switched to dynamic content in the late 1990s. While the mechanics of these attacks are still evolving, the bedrock error of improper or unsanitized user input has plagued web application security for decades.

QUALYS ID	TITLE
208001	A Link to a Malicious Page was Found
206011	A Malicious File Write was Detected
207003	A Match to a Known Virus was Detected
208000	Content was Loaded from a Remote Malicious Page
208002	Your Web Site Domain is Blacklisted
206012	A Malicious Process Launch Was Detected

Table 4: Threat Detections Discovered in 2022 by Web Application Scanning

Once exploited, web applications themselves can become tools of malicious actors via web malware. A survey of Qualys Web Malware Detection scans identified nearly 65,000 instances of malware in the dataset of 200,000 external-facing web applications used by Qualys customers. For these, adversaries inserted custom source code to infect client browsers with the goal of skimming payment card information, stealing credentials, mining cryptocurrency, sending users to blacklisted sites, and other nefarious actions. These attacks brought reputational damage and downstream implications to the organization and website visitors.

RISK FACT 5

5 INFRASTRUCTURE MISCONFIGURATIONS OPEN THE DOOR TO RANSOMWARE

Misconfigurations – errors that are unintended actions by an internal party — make up a large part of weaknesses in web applications and are one of the top reasons for data breaches. This is evidenced by the regular cadence of news around data leakage because of storage buckets or databases that were mistakenly left accessible without passwords or encryption.

Misconfigurations profoundly affect the security of an organization's cloud infrastructure. Findings for Risk Fact 5 begin with how Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure controls are performing against the Center for Internet Security (CIS) benchmarks. These control benchmarks help guide organizations to secure their part of the shared security responsibility model.

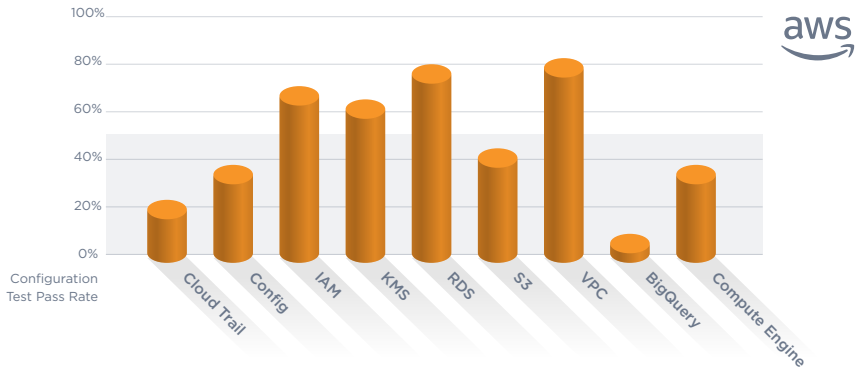


Figure 16: AWS Control Pass Rates in 2022

Data exfiltration due to misconfiguration in S3 buckets is a serious concern as it can result in high-profile security breaches. The weak access controls in Amazon S3 cloud storage buckets have been a major contributor to these incidents. The CIS Benchmark provides several security controls to measure public access to data in S3 buckets. While two of these controls, which check for public access to S3 buckets, perform well with only 1% of buckets being publicly exposed, there are two preventative controls that are implemented only 50% of the time. This means that there is a high potential for someone to inadvertently make an S3 bucket public.

Although protecting the entire bucket is crucial, it is also essential to safeguard the files stored in the bucket from being publicly accessible. Unfortunately, only 40% of organizations are currently utilizing preventative controls to prevent files from being accessed publicly. This leaves a significant portion of S3 buckets at risk of being misconfigured and exposes sensitive data to potential breaches. Therefore, it is crucial to educate organizations and individuals on the importance of proper configuration and security measures for S3 buckets to prevent data exfiltration and potential security incidents.

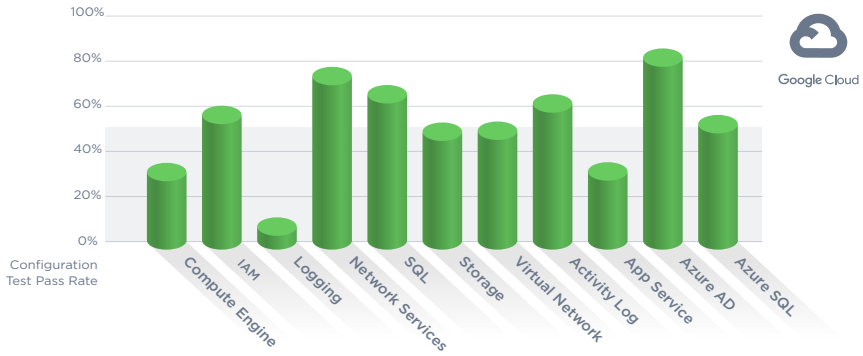


Figure 17: GCP Control Pass Rates in 2022

Within GCP, the data shows concerns with BigQuery configurations. The large cloud datasets housed in BigQuery are often used for AI/ML model training, which can contain sensitive information that could be exposed like S3's scenario described above. During 2022, 99% of the checks passed, ensuring that BigQuery datasets are not anonymously or publicly available.

Another observation is the failure to utilize customer-managed keys to encrypt data. On GCP, cloud service provider keys are used for encryption only 1% of the time. Not using customer-managed keys for encryption can pose a significant risk to the security of your data. While it's better to encrypt data using cloud service provider (CSP) keys than not to encrypt it at all, this method does not provide significantly stronger protection. If your data is encrypted using CSP keys and any of your identities are compromised, threat actors can use those privileges to gain access to your encrypted data. However, if you use your own encryption key, it adds an additional layer of protection. In this case, the threat actor would need access to the encryption key to decrypt the data.

From a security perspective, it is highly recommended to use customer-managed keys for encryption. By doing so, you maintain complete control over the encryption process and can ensure that your data remains secure. With customer-managed keys, you can encrypt your data with your own unique key, making it much more difficult for unauthorized individuals to access your sensitive information. Therefore, it's crucial to prioritize using customer-managed keys for encryption to minimize the risks of data breaches and ensure the highest level of security for your data.

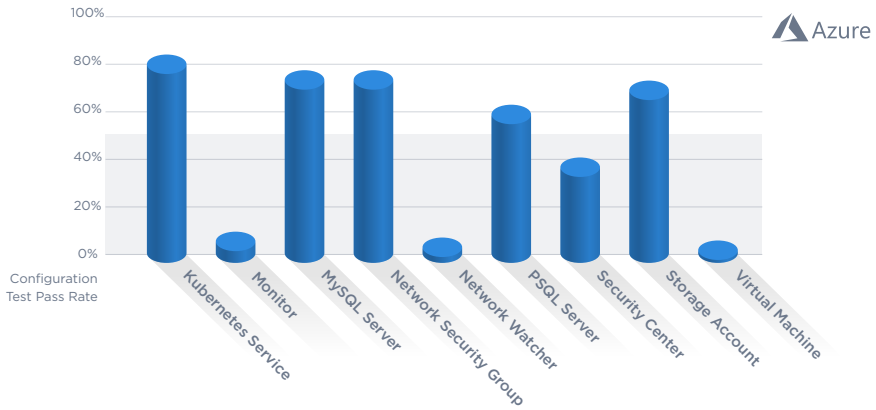


Figure 18: Azure Control Pass Rates in 2022

Similarly with Microsoft Azure, encryption is a group of controls that often fails. The Disks category has two checks failing 99% of its scans. These two settings are: "Ensure that 'OS and Data' disks are encrypted with Customer Managed Key" and "Ensure that all unattached VM disks are encrypted." Besides SQL Database Encryption (97.8% passing) and Web Apps using the latest version of TLS (85.4% passing), encryption checks are failing more than half of the time across the board.

On-Premises Misconfigurations

Security practitioners must also assess risks for on-premises misconfigurations. Qualys Cloud Platform controls enable the assessment of more than 100,000 potential misconfigurations that could weaken cloud security. Urgent attention should be given to the most prevalent misconfigurations. During 2022, the top 10 failing controls (see Table 5) were for password settings, user permissions, and protocols for Windows Updates.

CONTROL TITLE	PASS RATE
Ensure 'Always install with elevated privileges' is set to 'Disabled'	3.17%
Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	9.77%
Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	10.50%
Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	18.11%
Ensure 'Minimum password length' is set to '14 or more character(s)'	18.35%
Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	21.20%
Ensure 'Configure Automatic Updates' is set to 'Enabled'	22.07%
Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	28.94%
Ensure 'Enforce password history' is set to '24 or more password(s)'	36.55%
Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	36.75%

Table 5: Top 10 Misconfigurations for On-Premises Infrastructure

Linking Misconfigurations to Ransomware

In a joint effort between the MITRE Center for Threat Informed Defense and participating organizations, security controls were linked to MITRE ATT&CK Techniques and Mitigations to better understand their security coverage against threats outlined in the ATT&CK knowledge base. For this study, TRU examined all controls failing more than 50% of their scans and the associated MITRE ATT&CK techniques linked to those specific controls.

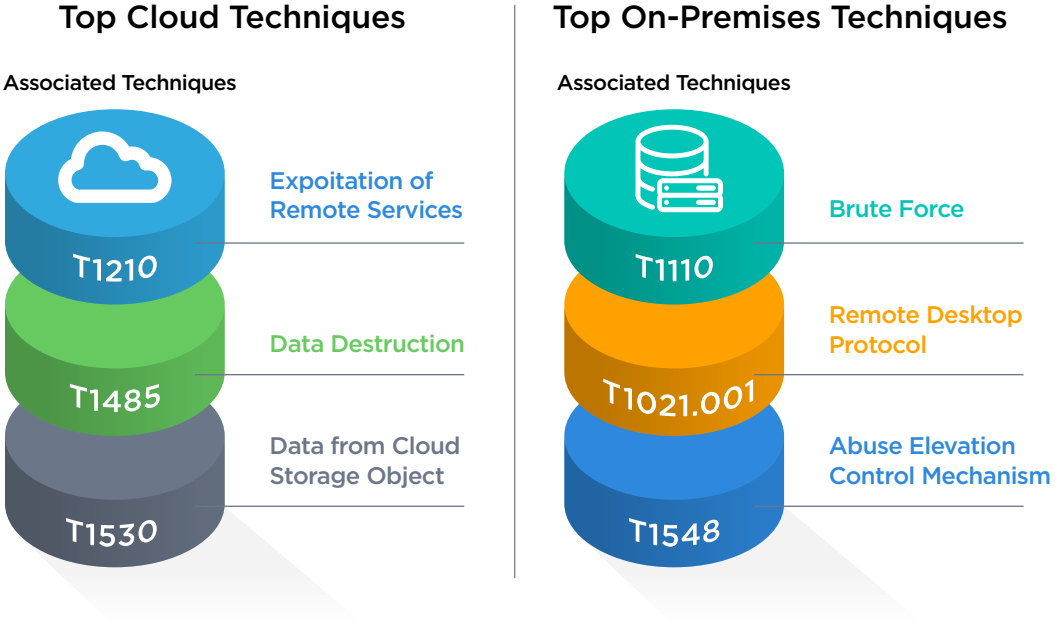


Figure 19: Typical Misconfigurations Leading to Ransomware

For cloud misconfigurations, the top three techniques associated with failing controls were T1210: Exploitation of Remote Services, 1485: Data Destruction, and 1530: Data from Cloud Storage Object. This indicates misconfigurations in the cloud are exposing organizations to exploitation, encryption, and exfiltration. These three techniques describe exactly how ransomware operates today.

Failing on-premises misconfigurations are associated with T1110: Brute Force, T1021.001: Remote Desktop Protocol, and T1548: Abuse Elevation Control Mechanism. When combined, these enable an attacker using guessed or stolen passwords to log into an exposed Remote Desktop Protocol (RDP) machine and elevate their privileges. This is a primary attack vector for Initial Access Brokers as an entry point into their intended victims.

Ransomware-Specific Misconfigurations

Configuration checks to prevent ransomware are useful when using the Qualys Best Practice Controls for Reducing Risk Related to Malware/Ransomware policy. During 2022, these misconfigurations failed half of their scans with a pass rate of 49.4%. Surprisingly, nearly a quarter of the tests received a 100% pass rate, which is great news. Failing misconfigurations are associated with enabling threat actors to move laterally within an organization.

The study applied this ransomware policy to a default installation of Windows 10 to compare it to the overall status across the anonymized data analyzed for this report. A default Windows 10 installation had a passing rate of 34%, so Qualys users have improved their security posture by an average of 15 percentage points.

TRU's evaluation discovered there are five settings securely configured in a default Windows 10 installation with a fail rate of more than 50%, meaning many organizations have intentionally misconfigured these settings. The top two failing controls were settings specific to Attack Surface Reduction, which indicates organizations are likely relying on other security tools to help prevent phishing-related attacks. The remaining three are password and RDP settings, which align with the overall failure rates of on-premises controls; these allow passwords to be used longer and changed less often while exposing RDP. While a valuable tool for administrators, there is potential for abuse — especially if connected directly to the internet.

CONTROL TITLE	PASS RATE	IMPACT
Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is 'configured'	0.47%	Phishing Attacks
Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	8.05%	Phishing Attacks
Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	15.75%	Password Stealing
Ensure 'Enforce password history' is set to '24 or more password(s)'	28.95%	Password Stealing
Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'	47.1%	Lateral Movement

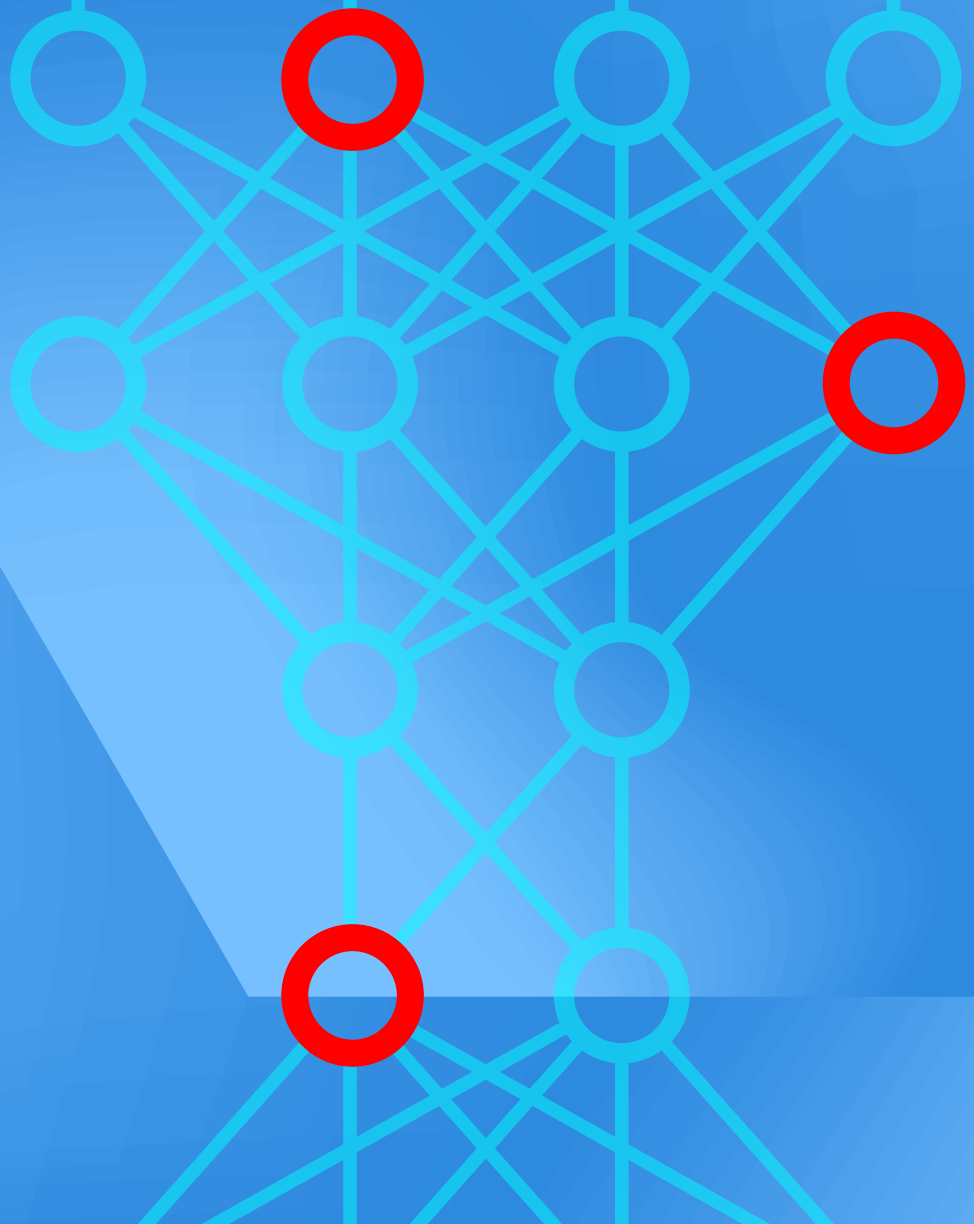
Table 6: Pass Rates for 5 Default Settings in Windows 10 During 2022

The good news is there are more settings that organizations are intentionally configuring correctly. These include 16 settings that are misconfigured by default — settings that organizations are correctly configuring more than 50% of the time to be more secure. We can see quite a few configurations dealing with passwords, even though a few are intentionally misconfigured. At a high level, many of these are dealing with brute force/password stealing and lateral movement. Controls such as Universal Naming Convention (UNC) paths, Network Access, and Windows Firewall will reduce the ability of threat actors to laterally move within the environment. The password settings enable protections to prevent a threat actor from successfully achieving brute force of passwords by increasing the complexity and having thresholds automatically locking out the process upon invalid login attempts.

CONTROL TITLE	PASS RATE	IMPACT
Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON shares'	51.47%	Lateral Movement
Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all SYSVOL shares'	51.95%	Lateral Movement
Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	52.61%	Password Stealing
Inbound exceptions to the firewall on Windows domain workstations must only allow authorized remote management hosts.	52.84%	Lateral Movement
Outbound exceptions to the firewall on Windows domain workstations must only allow authorized remote management hosts.	52.84%	Lateral Movement
Ensure LAPS AdmPwd GPO Extension / CSE is installed	54.35%	Password Stealing
Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	55.24%	Escalating Privileges
Ensure 'Minimum password age' is set to '1 or more day(s)'	57.80%	Password Stealing
Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	61.42%	Lateral Movement
Ensure 'Enable Local Admin Password Management' is set to 'Enabled'	61.61%	Password Stealing
Ensure 'Password must meet complexity requirements' is set to 'Enabled'	67.09%	Password Stealing
Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	70.47%	Lateral Movement
Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	92.54%	Escalating Privileges
Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	93.65%	Password Stealing
Ensure 'Account lockout duration' is set to '15 or more minute(s)'	94.23%	Password Stealing
Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	94.72%	Password Stealing

Table 7: Pass Rates for 16 Default Settings in Windows 10 that Are Intentionally Configured Correctly

RECOMMENDATIONS



Recommendations

Threat actors remained highly adaptable in 2022, constantly tweaking their tactics, techniques and procedures to achieve their objectives. As we prepare for 2023 and beyond, defenders must evolve alongside the changing threat landscape and take action to reduce and manage risk in their environments. With our research yielding five of the most severe Risk Facts faced by organizations, below are immediate practices that security teams can implement to increase the resilience of their organization:

To reduce overall risk, leverage a threat-informed defensive strategy to prioritize vulnerability remediations.

With the exponential growth in vulnerabilities year over year, it is important to realize that only a subset of these introduces the most risk to an organization — e.g., first and foremost, those that are known to be actively exploited in the wild. Vulnerability management must move beyond sharing a long list of vulnerabilities to helping prioritize and create remediation plans. Risk-based vulnerability management gives security / IT teams a shared asset context and the ability to create workflows to quickly align and respond to threats. Incorporating threat intelligence sources in your vulnerability management program or platform is crucial to stay on top of the latest threats.

Rely on automation for patching vulnerabilities wherever possible.

By automating patching for software such as Microsoft Windows and Google Chrome, platforms and applications will quickly limit the ability for adversaries to exploit known vulnerabilities. Automation also allows organizations to focus personnel on manually patching the remaining systems in their environment and addressing those critical issues. Further, using a risk-based automation approach that considers intelligence on highly exploitable vulnerabilities overlayed with context from your environment reduces overall risk to your organization. In other words, patch what is exploitable on valuable systems, not what is merely vulnerable, and use automation where risk of breaking systems is lower.

Be wary of externally facing systems which are exploited for initial access.

Threat actors will persistently seek entry points in perimeter devices, with any exposed web application posing an immense level of risk. To mitigate this threat, organizations must reduce their unnecessary attack surface — e.g., the threat from "unknown unknowns" — as much as possible, by continuously monitoring their external attack surface, tracking changes and receiving notifications when new, unknown assets or critical issues are found and keeping systems up to date.

Web applications are a prime target for gaining a foothold or staging attacks.

Web apps often process or store sensitive information that threat actors would find valuable. Even non-critical systems can serve as a launch pad for an attack or store malicious tools for malicious campaigns against secondary victims. Therefore, scanning web applications for vulnerabilities and configuration issues is crucial to prevent attackers from exploiting them.

Configuration issues introduce the same level of risk as vulnerabilities.

A misconfigured system can be abused for various reasons, with many configuration issues seen in 2022 related to ransomware. Utilizing 'Level 1 of CIS Hardening Benchmarks' is an effective starting point to address this threat and improve security posture. Individual controls associated with ransomware-specific techniques — such as those mentioned throughout this report — must be reviewed carefully when found failing in your environment. Additionally, it is vital to understand the shared security model for cloud infrastructure. Leveraging the CIS Hardening Benchmarks or other best practices to protect cloud workloads will reduce the overall risk to your organization.

Qualys Products

Start a free trial to learn more:

VMDR **Vulnerability Management, Detection and Response (VMDR)**
qualys.com/try/vmdr

WAS **Web App Scanning (WAS)**
qualys.com/try/web-application-scanning

PC **Policy Compliance (PC)**
qualys.com/try/policy-compliance

EDR **Multi-Vector EDR**
qualys.com/try/endpoint-detection-response

TC **TotalCloud**
qualys.com/try/totalcloud

PM **Patch Management**
qualys.com/try/patch-management

ABOUT TRU

About the Qualys Threat Research Unit (TRU)

The Threat Research Unit (TRU) is the research arm of Qualys. The TRU team's focus is devoted to vulnerability, compliance, malware, and threat actor research with the goal of providing world-class security intelligence, detection data, and guidance for the Qualys Cloud Platform.

New technologies are revolutionizing lives and economies around the world. Cyberthreats are growing at a similar pace, endangering access to the services that improve lives everywhere. By empowering customers and stakeholders for IT, security and compliance with TRU research and insights, together we can secure and defend the digital world from bad actors who create chaos and erode trust. We are the Qualys Threat Research Unit. Our shield is your shield.

ABOUT QUALYS

About Qualys

Qualys, Inc. (NASDAQ: **QLYS**) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit **qualys.com**.

Learn More:

Company Website: qualys.com

Qualys Security Blog: blog.qualys.com

Follow Us:

LinkedIn

Twitter

Facebook

CONTRIBUTORS

Contributors to the 2023 Qualys TruRisk Research Report

Saeed Abbasi | Manager, Vulnerability Signatures

Irfan Asrar | Director, Threat Research

Parag Bajaria | VP, Cloud and Container Security Services

Dave Buerger | Editor

John Delaroderie | Director, Product Management - Web Application Security

Mayuresh Dani | Manager, Threat Research

Jackie Dutton | Public Relations Manager

Chaitanya Haritash | Malware Researcher

Aparna Hinge | Senior Manager - Compliance Research Analysis

Bharat Jogi | Director, Vulnerability Research

Eran Livne | Director, Product Management - Endpoint Remediation

Bajrang Mane | Manager, Malware Research

Ghanshyam More | Malware Researcher

Aubrey Perin | Lead Threat Intelligence Analyst

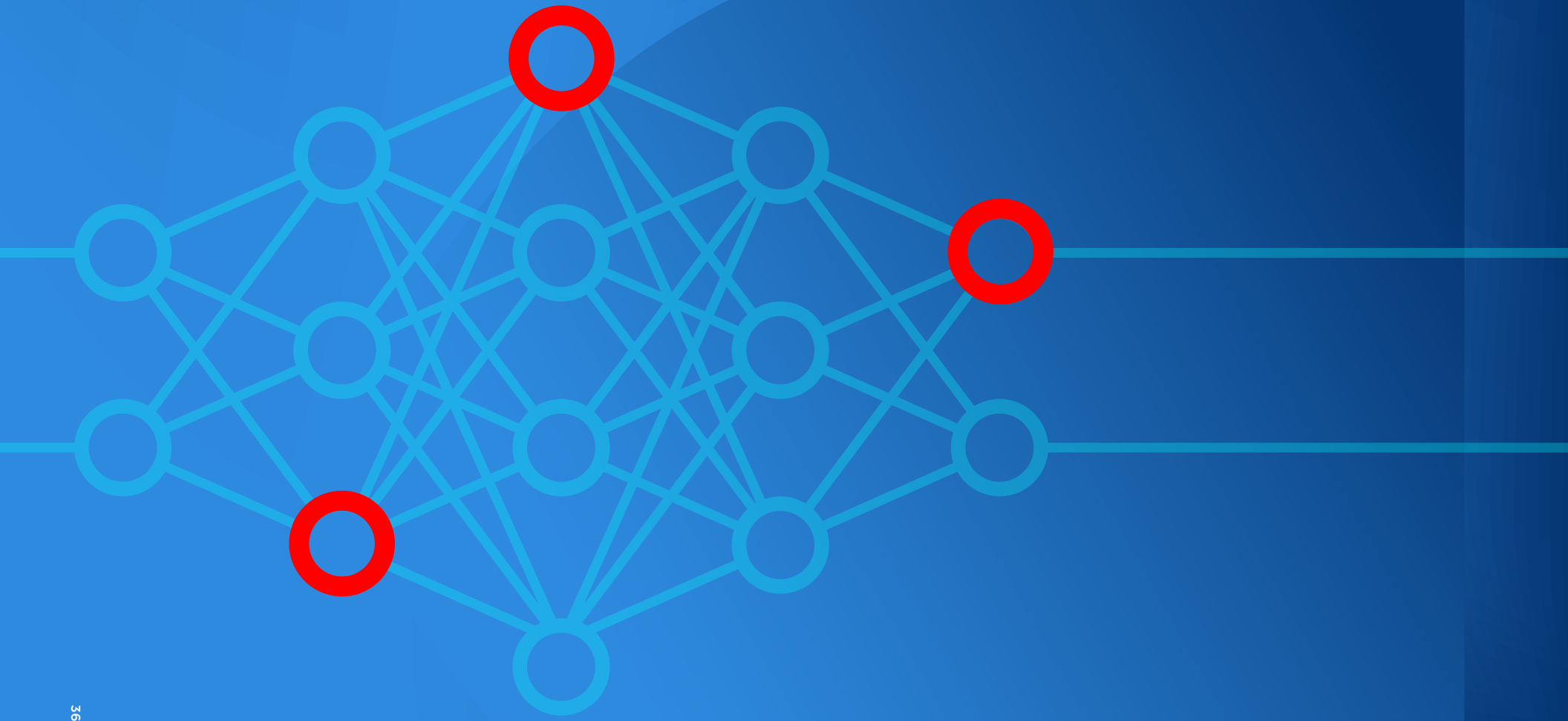
Mehul Revankar | VP, Product Management - VMDR

Sheela Sarva | Director, Web Application Security

Travis Smith | VP, Threat Research Unit

Ankur Tyagi | Principal Engineer, Threat Research

APPENDIX A



CVE LISTING

QUALYS ID	TITLE	QVS
CVE-2021-4034	polkit's pkexec Local Privilege Escalation Vulnerability (PwnKit)	95
CVE-2022-0028	Palo Alto Networks PAN-OS Reflected Amplification Denial-of-Service Vulnerability	95
CVE-2022-0543	Debian-specific Redis Server Lua Sandbox Escape Vulnerability	95
CVE-2022-0609	Google Chrome Animation Module Use-After-Free Vulnerability	95
CVE-2022-0824	webmin Improper Access Control to Remote Code Execution	75
CVE-2022-0847	Linux Kernel Privilege Escalation Vulnerability in push_pipe Function (Dirty Pipe)	95
CVE-2022-0995	Linux Kernel Event Notification Subsystem Out-of-Bounds Write Flaw	75
CVE-2022-1040	Sophos Firewall User Portal and Webadmin Authentication Bypass Vulnerability	100
CVE-2022-1096	Google Chromium V8 Type Confusion Vulnerability	95
CVE-2022-1329	WordPress Elementor Website Builder Plugin Remote Code Execution Vulnerability	75
CVE-2022-1364	Google Chromium V8 Turbofan Type Confusion Vulnerability	95
CVE-2022-1388	F5 BIG-IP Missing Authentication Vulnerability	95
CVE-2022-2003	AutomationDirect DirectLOGIC Sensitive Information Leakge Vulnerability	65
CVE-2022-20699	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	95
CVE-2022-20700	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	95
CVE-2022-20701	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	95
CVE-2022-20703	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	95
CVE-2022-20708	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	95
CVE-2022-20821	Cisco IOS XR Open Port Vulnerability	95
CVE-2022-20828	Cisco Adaptive Security Appliance (ASA) FirePOWER Arbitrary Command Execution Vulnerability	75
CVE-2022-2143	Advantech iView NetworkServlet Command Injection Vulnerability	75
CVE-2022-21882	Microsoft Win32k Privilege Escalation Vulnerability	95
CVE-2022-21919	Microsoft Windows User Profile Service Privilege Escalation Vulnerability	95
CVE-2022-21971	Microsoft Windows Runtime Remote Code Execution Vulnerability	95
CVE-2022-21999	Windows Print Spooler Privilege Escalation Vulnerability (SpoolFool)	95
CVE-2022-22047	Microsoft Windows Client Server Runtime Subsystem (CSRSS) Privilege Escalation Vulnerability	95
CVE-2022-22536	SAP Multiple Products HTTP Request Smuggling Vulnerability	95

QUALYS ID	TITLE	QVS
CVE-2022-22587	Apple Multiple Products Memory Corruption Vulnerability	95
CVE-2022-22616	Apple Multiple Products Gatekeeper Bypass Incorrect Authorization Vulnerability	40
CVE-2022-22620	Apple Webkit Remote Code Execution Vulnerability	95
CVE-2022-22674	Apple macOS Out-of-Bounds Read Vulnerability	95
CVE-2022-22675	Apple macOS Out-of-Bounds Write Vulnerability	95
CVE-2022-22718	Windows Print Spooler Privilege Escalation Vulnerability (SpoolFool)	95
CVE-2022-2294	WebRTC Heap Buffer Overflow Vulnerability	95
CVE-2022-22947	VMware Spring Cloud Gateway Code Injection Vulnerability	95
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability	100
CVE-2022-22960	VMware Multiple Products Privilege Escalation Vulnerability	95
CVE-2022-22963	VMware Tanzu Spring Cloud Function Remote Code Execution Vulnerability	95
CVE-2022-22965	Spring Framework JDK 9+ Remote Code Execution Vulnerability (Spring4Shell)	100
CVE-2022-22972	VMware Multiple Products Authentication Bypass Vulnerability	75
CVE-2022-22973	VMware Workspace ONE Access and Identity Manager Privilege Escalation Vulnerability	75
CVE-2022-23131	Zabbix Frontend Authentication Bypass Vulnerability	95
CVE-2022-23134	Zabbix Frontend Improper Access Control Vulnerability	95
CVE-2022-23176	WatchGuard Firebox and XTM Privilege Escalation Vulnerability	95
CVE-2022-23277	Microsoft Exchange Server Remote Code Execution Vulnerability	75
CVE-2022-23642	Sourcegraph gitserver Service Remote Code Execution Vulnerability	75
CVE-2022-23812	node-ipc Malicious peacenotwar Package Import Code Injection Vulnerability	95
CVE-2022-24086	Adobe Commerce and Magento Open Source Improper Input Validation Vulnerability	95
CVE-2022-24112	Apache APISIX Authentication Bypass Vulnerability	96
CVE-2022-24521	Microsoft Windows CLFS Driver Privilege Escalation Vulnerability	95
CVE-2022-24664	PHP Everywhere WordPress metaboxes Code Injection Vulnerability	41
CVE-2022-24665	PHP Everywhere WordPress gutenberg Code Injection Vulnerability	41
CVE-2022-24682	Zimbra Webmail Cross-Site Scripting Vulnerability	95
CVE-2022-24706	Apache CouchDB Insecure Default Initialization of Resource Vulnerability	95

QUALYS ID	TITLE	QVS
CVE-2022-24734	MyBB Admin Control Code Injection Remote Code Execution Vulnerability	75
CVE-2022-24934	Kingsoft WPS Office wpsupdater.exe Remote Code Execution Vulnerability	95
CVE-2022-25075	TOTOLink A3000RU Command Injection Vulnerability	71
CVE-2022-25076	TOTOLink A800R Command Injection Vulnerability	71
CVE-2022-25077	TOTOLink A3100R Command Injection Vulnerability	71
CVE-2022-25078	TOTOLink A3600R Command Injection Vulnerability	71
CVE-2022-25079	TOTOLink A810R Command Injection Vulnerability	71
CVE-2022-25080	TOTOLink A830R Command Injection Vulnerability	71
CVE-2022-25081	TOTOLink T10 Command Injection Vulnerability	71
CVE-2022-25082	TOTOLink A950RG Command Injection Vulnerability	71
CVE-2022-25083	TOTOLink A860R Command Injection Vulnerability	71
CVE-2022-25084	TOTOLink T6 Command Injection Vulnerability	72
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	100
CVE-2022-26138	Atlassian Questions For Confluence App Hard-coded Credentials Vulnerability	94
CVE-2022-26143	MiCollab and MiVoice Business Express TP-240 Component Access Control Vulnerability	95
CVE-2022-26186	TOTOLink N600R Command Injection Vulnerability	71
CVE-2022-26210	TOTOLink Multiple Firmware Versions Command Injection Vulnerability	71
CVE-2022-26258	D-Link DIR-820L Remote Code Execution Vulnerability	95
CVE-2022-26318	WatchGuard Firebox and XTM Appliances Arbitrary Code Execution	95
CVE-2022-26352	dotCMS Unrestricted Upload of File Vulnerability	100
CVE-2022-26485	Mozilla Firefox Use-After-Free Vulnerability	95
CVE-2022-26486	Mozilla Firefox WebGPU IPC Framework Use-After-Free Vulnerability	95
CVE-2022-26500	Veeam Backup & Replication Remote Code Execution Vulnerability	95
CVE-2022-26501	Veeam Backup & Replication Remote Code Execution Vulnerability	93
CVE-2022-26504	Veeam Backup & Replication Improper Authentication Vulnerability	95
CVE-2022-26706	Apple Multiple Products Sandbox Bypass Vulnerability	36
CVE-2022-26871	Trend Micro Apex Central Arbitrary File Upload Vulnerability	95

QUALYS ID	TITLE	QVS
CVE-2022-26904	Microsoft Windows User Profile Service Privilege Escalation Vulnerability	95
CVE-2022-26923	Active Directory Domain Services Elevation of Privilege Vulnerability (Certifried)	95
CVE-2022-26925	Windows LSA Spoofing Vulnerability (PetitPotam)	95
CVE-2022-27226	iRZ Mobile Router Cross Site Request Forgery Remote Code Execution Vulnerability	72
CVE-2022-27518	Citrix Application Delivery Controller (ADC) and Gateway Authentication Bypass Vulnerability	95
CVE-2022-27593	QNAP Photo Station Externally Controlled Reference Vulnerability	93
CVE-2022-27666	Linux Kernel IPsec ESP Transformation Out-of-Bounds Write Privilege Escalation Vulnerability	75
CVE-2022-27924	Zimbra Collaboration (ZCS) Command Injection Vulnerability	95
CVE-2022-27925	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	95
CVE-2022-28219	ManageEngine ADAudit Plus Path Traversal XML Injection Vulnerability	75
CVE-2022-28381	ALLMediaServer Buffer Overflow Vulnerability	75
CVE-2022-2856	Google Chrome Intents Insufficient Input Validation Vulnerability	95
CVE-2022-28810	Zoho ManageEngine ADSelfService Plus Remote Code Execution Vulnerability	95
CVE-2022-28958	D-Link DIR-816L Remote Code Execution Vulnerability	95
CVE-2022-29464	WSO2 Multiple Products Unrestrictive Upload of File Vulnerability	100
CVE-2022-29499	Mitel MiVoice Connect Data Validation Vulnerability	100
CVE-2022-29806	ZoneMinder Language Settings Remote Code Execution Vulnerability	75
CVE-2022-30170	Windows Credential Roaming Service Elevation of Privilege Vulnerability	95
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	100
CVE-2022-30333	RARLAB UnRAR Directory Traversal Vulnerability	95
CVE-2022-30525	Zyxel Multiple Firewalls OS Command Injection Vulnerability	95
CVE-2022-30526	Zyxel Firewall SUID Binary Privilege Escalation Vulnerability	75
CVE-2022-3075	Google Chromium Insufficient Data Validation Vulnerability	95
CVE-2022-30781	Gitea Git Fetch Remote Code Execution Vulnerability	75
CVE-2022-31137	Roxy-WI subprocess_execute Function Remote Command Execution Vulnerability	75
CVE-2022-31199	Netwrix Auditor User Activity Video Recording Component Remote Code Execution Vulnerability	90
CVE-2022-31460	Meeting Owl Pro and Whiteboard Owl Hard-Coded Credentials Vulnerability	95

QUALYS ID	TITLE	QVS
CVE-2022-31625	PHP Multiple Versions pg_query_params Function Remote Code Execution Vulnerability	41
CVE-2022-31626	PHP Multiple Versions pdo_mysql Extension Remote Code Execution Vulnerability	41
CVE-2022-31660	VMware Workspace ONE Access, Identity Manager and vRealize Automation Privilege Escalation Vulnerability	75
CVE-2022-31814	pfSense pfBlockerNG Remote Code Execution Vulnerability	75
CVE-2022-3218	Necta LLC WiFi Mouse Authentication Bypass Vulnerability	75
CVE-2022-3229	Unified Intents Unified Remote Protocol Authentication Bypass Vulnerability	75
CVE-2022-3236	Sophos Firewall Code Injection Vulnerability	95
CVE-2022-32893	Apple iOS and macOS Out-of-Bounds Write Vulnerability	95
CVE-2022-32894	Apple iOS and macOS Out-of-Bounds Write Vulnerability	95
CVE-2022-32917	Apple iOS, iPadOS, and macOS Remote Code Execution Vulnerability	95
CVE-2022-33891	Apache Spark Command Injection Vulnerability	95
CVE-2022-34151	OMRON Corporation Multiple Products Credentials Leak Vulnerability	95
CVE-2022-34538	Digital Watchdog DW MEGApix IP Camera Command Injection Vulnerability	35
CVE-2022-34713	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (DogWalk)	95
CVE-2022-34721	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	95
CVE-2022-34918	Linux Kernel Netfilter nft_set_elem_init Heap Overflow Privilege Escalation Vulnerability	75
CVE-2022-35405	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	95
CVE-2022-35526	WAVLINK login.cgi Command Injection Vulnerability	71
CVE-2022-3569	Zimbra Collaboration Suite (ZCS) sudo Privilege Escalation Vulnerability	75
CVE-2022-35914	Teclib GLPI Remote Code Execution Vulnerability	95
CVE-2022-36267	Airspan AirSpot 5410 Remote Command Injection Vulnerability	75
CVE-2022-36446	Webmin software/apt-lib.pl Command Injection Vulnerability	75
CVE-2022-36534	Syncovery For Linux Web-GUI Authenticated Remote Command Execution Vulnerability	75
CVE-2022-36536	Syncovery For Linux post_applogin.php Component Privilege Escalation Vulnerability	75
CVE-2022-36804	Atlassian Bitbucket Server and Data Center Command Injection Vulnerability	95
CVE-2022-37042	Zimbra Collaboration (ZCS) Authentication Bypass Vulnerability	95
CVE-2022-37061	FLIR AX8 Remote Command Injection Vulnerability	75

QUALYS ID	TITLE	QVS
CVE-2022-3723	Google Chromium V8 Type Confusion Vulnerability	95
CVE-2022-37393	Zimbra's sudo Configuration Privilege Escalation Vulnerability	75
CVE-2022-37706	Enlightenment Window Manager enlightenment_sys Component Privilege Escalation Vulnerability	95
CVE-2022-37969	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	95
CVE-2022-40139	Trend Micro Apex One and Apex One as a Service Improper Validation Vulnerability	95
CVE-2022-40684	Fortinet Multiple Products Authentication Bypass Vulnerability	95
CVE-2022-41033	Microsoft Windows COM+ Event System Service Privilege Escalation Vulnerability	95
CVE-2022-41040	Microsoft Exchange Server Elevation of Privilege Vulnerability (ProxyNotShell)	95
CVE-2022-41049	Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability	95
CVE-2022-41073	Microsoft Windows Print Spooler Privilege Escalation Vulnerability	95
CVE-2022-41080	Microsoft Exchange Server Privilege Escalation Vulnerability (OWASSRF)	100
CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability (ProxyNotShell)	95
CVE-2022-41091	Windows Mark of the Web Security Feature Bypass Vulnerability	95
CVE-2022-41099	BitLocker Security Feature Bypass Vulnerability	30
CVE-2022-41125	Microsoft Windows CNG Key Isolation Service Privilege Escalation Vulnerability	95
CVE-2022-41128	Microsoft Windows Scripting Languages Remote Code Execution Vulnerability	95
CVE-2022-41343	Dompdf FontMetrics.php Remote File Inclusion Vulnerability	42
CVE-2022-4135	Google Chromium Heap Buffer Overflow Vulnerability	95
CVE-2022-41352	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	95
CVE-2022-41622	BIG-IP and BIG-IQ iControl SOAP Cross-Site Request Forgery Vulnerability	75
CVE-2022-41800	BIG-IP iControl REST Endpoint Command Injection Vulnerability	75
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	95
CVE-2022-4262	Google Chromium V8 Type Confusion Vulnerability	95
CVE-2022-42827	Apple iOS and iPadOS Out-of-Bounds Write Vulnerability	95
CVE-2022-42856	Apple iOS Type Confusion Vulnerability	95
CVE-2022-44698	Microsoft Defender SmartScreen Security Feature Bypass Vulnerability	95
CVE-2022-45045	Xiongmai NVR Multiple Devices Arbitrary Command Execution Vulnerability	41
CVE-2022-45359	YITH WooCommerce Gift Cards Premium Plugin Arbitrary File Upload Vulnerability	95