2022 Vulnerability Intelligence Report

Caitlin Condon, Senior Manager, Security Research, Rapid7
Ron Bowes, Lead Security Researcher, Rapid7
Erick Galinkin, Principal AI Researcher, Rapid7

RAPID7

CONTENTS

Executive Summary 3

Big Picture 5

2022 Exploited and Significant Vulnerabilities 8

- Widespread Threats 9
  - We Need to Talk About Exchange (Again) 14
- Other Known Exploited Vulnerabilities 16
  - Spotlight: ManageEngine ADSelfService Plus CVE-2022-28810 19
- Impending Threats 20
  - 2020 and 2021 Impending Threats: Where Are They Now? 21

Notable Attack Trends 23

- Time to Exploitation 23
- Ransomware 26
- Attacker Utilities and Vulnerability Classes 30
- Spotlight: Privilege Escalation from the Perimeter 33

Conclusion 35

- Future Rapid7 Research 36

Appendix 37

- Full 2022 Dataset 37
- Notes on Methodology 41
  - Threat Categorization 41
  - Ransomware Citations 42
  - Calculating Time to Known Exploitation (TTKE) 42
- Glossary of Terms 43
  - Attacker Utilities 43
  - Vulnerability Classes 44

References 46

EXECUTIVE SUMMARY

Security, IT, and other teams tasked with vulnerability management and risk reduction operate in high-urgency, high-stakes environments where informed decision-making hinges on the ability to quickly find signal in a sea of perpetual noise. When a new potential threat emerges, information security professionals often find themselves needing to translate vague descriptions and untested research artifacts into actionable intelligence for their own particular risk models.

> **Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions, and share information on why certain flaws are more likely to be exploited than others.**

Rapid7's Vulnerability Intelligence Report examines notable vulnerabilities and high-impact attacks from 2022 in order to highlight exploitation trends, explore attacker use cases, and offer a framework for understanding new security threats as they arise. Our aim is to contextualize the vulnerabilities that introduce serious risk to a wide range of organizations.

The report examines 50 vulnerabilities that pose considerable risk to organizations of all sizes. In total, this report includes 45 vulnerabilities that were exploited in the wild in 2022, of which 44% arose from zero-day exploits. See our appendix for additional context on vulnerability selection.

2022 findings include:

Widespread exploitation of new vulnerabilities decreased somewhat in 2022, but broad, opportunistic attacks still drove considerable risk. Rapid7's vulnerability research team tracked **28** net-new widespread threats in 2022, a **15%** decrease in widespread threats from 2021.

Zero-day exploitation was still a significant threat in 2022, though we saw a modest decline in mass zero-day attacks. **43%** of the widespread threats Rapid7 researchers analyzed in 2022 began with a zero-day exploit, down from **52%** in 2021.

Attackers are still developing and deploying exploits faster than ever. **56%** of the vulnerabilities in this report were exploited within seven days of public disclosure — a **12%** rise over 2021 and an **87%** rise over 2020.

Only **14** of the vulnerabilities in this report are known to have been exploited to carry out ransomware attacks — a significant **(33%)** decrease from 2021 despite consistent ransomware activity. This may indicate that ransomware operations have become less reliant on new vulnerabilities, but it may also stem from other factors, like lower reporting of ransomware incidents.

Other vulnerability and exploit trends examined in this report include ransomware ecosystem complexity, privilege escalation from the network perimeter, and the long tail of exploitation across older vulnerabilities.

The full 2022 dataset is available in the appendix.

Big Picture

The past three years have witnessed a convergence of major attack trends that shaped the security landscape with blunt force. Zero-day exploitation hit an all-time high in 2021, ransomware business models matured and expanded with devastating effect, and organizations were plagued by widespread attacks on business-critical technologies. For many, 2021 was a sledgehammer — not always terribly sophisticated, but undeniably effective at distributing damage across a broad area.

The security landscape in 2022 has been marked by more nuance. Zero-day exploitation seems to have plateaued at high elevation, but zero-day exploits morphed into mass exploitation events less frequently than they did in 2021. The volume of ransomware incidents continued to rise, but there are fewer CVEs mapped directly to ransomware in our 2022 report data than there were in 2021.

Finally, as always, we saw celebrity vulnerabilities and hotly anticipated security releases whose practical impact ended up being rather low — but impracticality failed to deter attackers from indiscriminately lobbing exploits at internet-accessible targets, searching in vain for vulnerable code paths that often failed to materialize. In other words, definitively classifying and communicating risk was more complex in 2022, even for research teams whose bread and butter is vulnerability and exploit intelligence.

> **Many organizations spent the first weeks (or months) of 2022 working their way down a lengthy list of Log4Shell remediations, taxing IT and security team resources that had already been depleted by shrinking budgets and pandemic exhaustion.**

Despite the vulnerability's undeniable impact, it turned out to be somewhat overrated as a universal attack vector; instead, application-specific exploits had to be crafted for valuable target technologies, a number of which fell prey to Log4Shell exploitation in January 2022 and beyond. A months-long tail of vendor impact assessments and downstream patches — many of which required constant monitoring of advisories and community forums — also compounded vulnerability management challenges for overburdened IT security teams.

The security landscape in 2022 was not shaped by Log4Shell alone, of course, just as 2021's threat landscape featured dozens of widely exploited flaws and high-profile attacks before December 9 rolled around. But the vulnerability that the U.S. Cyber Safety Review Board (CSRB) called "endemic" did set the stage for community-wide vulnerability response in 2022 in several key ways.

First, Log4Shell trauma put businesses in a heightened state of ready alert, driving stronger-than-usual reactions to subsequent vulnerabilities in popular libraries and frameworks. Neither "Spring4Shell" nor the not-so-aptly named "Text4Shell" merited its moniker, for instance. Moreover, the opportunity cost of an all-consuming response to a vulnerability like Spring4Shell turned out to be high: Between March 25 and April 6, 2022, seven different vulnerabilities that eventually saw significant exploitation came to light, including three zero-day flaws and a critical VMware attack chain that was exploited for full system takeover within 48 hours of disclosure. In hindsight, any number of these other flaws was arguably more urgent than Spring4Shell, but Log4Shell response syndrome meant that organizations — including security companies — sunk resources disproportionately into vulnerabilities that looked similar to CVE-2021-44228 on the surface, delaying or deprioritizing mitigations for other issues.

Log4Shell's dragging tail of downstream advisories also served to emphasize the importance of transparent, timely, standardized vulnerability disclosure practices in a healthy security ecosystem. There were plenty of software producers whose teams worked overtime to assess and communicate Log4Shell impact clearly in the days and weeks following the incident, but there were also plenty of cases where security teams were left wondering about uncommunicated risk. While there are a few technology vendors that embrace plain-spoken frankness about vulnerabilities, the industry has plenty more ground to cover to ensure there are clear-cut, openly accessible security advisories that include technical vulnerability details, attack scenarios, and timelines of exploitation. In a persistently elevated threat climate, with overt dependencies on common frameworks and shared components, transparency and useful intelligence sharing should be the ground floor, not the ceiling.

Admittedly, doing all this well requires an abundance of security expertise. In an uneasy socioeconomic climate, concurrent crises are a stark reminder that markets depend on people to drive innovation and uphold critical infrastructure, as our strained healthcare systems have demonstrated so plainly these past few years. When droves of security practitioners are at risk of succumbing to burnout, we face an intersectional dilemma with broad business implications.

> **In an industry captivated by the promises and potential of advanced technology, it can be easy to forget that the fundamental practice of security is not merely mechanical, but creative. It requires the ability to make connections, to think ahead, and above all, to make informed decisions when "risk" is a value constantly in flux.**

As ever, this report strives to provide a framework for risk-based decision making, backed by both original analysis from Rapid7 research teams and robust, well-documented third-party sources.

2022 Exploited and Significant Vulnerabilities

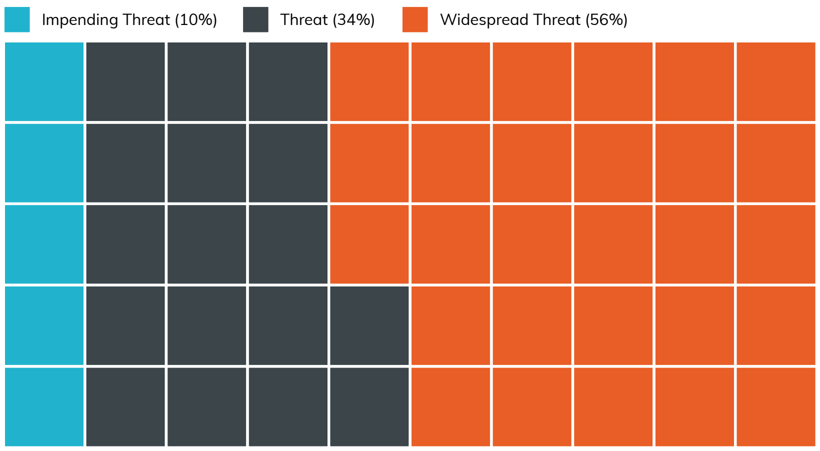
Rapid7 vulnerability researchers prioritize CVEs that are likely to impact many organizations, instead of those likely to affect only a few. We intentionally differentiate mass attacks from smaller-scale or targeted exploitation; when a vulnerability is exploited by many attackers across many different industries and organizations, we deem that vulnerability a **widespread threat**. As a rule, organizations should expect to conduct incident response investigations that look for IOCs and post-exploitation activity during widespread threat events in addition to activating emergency patching protocols.

Vulnerabilities categorized as **threats** have been confirmed to be exploited in the wild by reputable sources (including Rapid7's own Labs and services teams), but in a more limited or targeted fashion than CVEs classified as widespread threats. **Impending threats**, on the other hand, have not yet seen exploitation by adversaries, but in our view are likely and valuable attack targets.

What is a threat?

A threat exists when there is an adversary with the intent, capability, and opportunity to act. When only two of these elements are present (e.g., intent and opportunity), we call it an impending threat. When just one element is present (e.g., an opportunity in the form of a vulnerability), it is a potential threat.

2022 Vulnerabilities by Threat Status



Widespread Threats

Once again, widespread threats comprised the majority of our 2022 vulnerability dataset (56%), down from 66% in 2021. Common payloads dropped during mass exploitation included cryptocurrency miners, web shells, and a variety of botnet malware in addition to an ever more diverse set of ransomware payloads. At time of writing, all of the CVEs listed below except one (CVE-2022-33891) were on the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) list.

Table 1: 2022 widely exploited vulnerabilities

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2021-20038 SonicWall SMA 100 Series Unauthenticated Stack-Based Buffer Overflow	Threat - widespread	9*	Network pivot	Memory Corruption
CVE-2021-44228 Log4Shell Remote Code Execution in VMware vCenter Server and VMware Horizon	Threat - widespread	26	Remote code execution	Injection
CVE-2021-21882 Microsoft Windows Win32k Elevation of Privilege	Threat - widespread (0 day)	0	Local code execution	Memory Corruption
CVE-2021-4034 "Pwnkit" Linux Local Privilege Escalation	Threat - widespread	153	Local code execution	Memory Corruption
CVE-2022-22947 Spring Cloud Gateway Code Injection Vulnerability	Threat - widespread	34	Cloud infrastructure compromise	Injection
CVE-2022-26352 dotCMS Directory Traversal Remote Code Execution	Threat - widespread	Unknown	Remote code execution	Improper Access Control
CVE-2022-22963 Spring Cloud Function Unauthenticated Remote Code Execution (SpEL injection)	Threat - widespread (0day)	0	Cloud infrastructure compromise	Injection
CVE-2022-27925 Zimbra Collaboration Suite Directory Traversal	Threat - widespread	120	Remote code execution	Improper Access Control

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-22954 VMware Workspace ONE Access / Identity Manager Remote Code Execution	Threat - widespread	2	Cloud infrastructure compromise	Injection
CVE-2022-22960 VMware Workspace ONE Access/Identity Manager Local Privilege Escalation	Threat - widespread	2	Local code execution	Improper Access Control
CVE-2022-29464 WSO2 File Upload Remote Code Execution	Threat - widespread	4	IT security management compromise	Injection
CVE-2022-29499 Mitel MiVoice Connect Service Appliance Data Validation Vulnerability	Threat - widespread (0 day)	0	Network pivot	Injection
CVE-2022-1388 F5 BIG-IP iControl REST Authentication Bypass (RCE)	Threat - widespread	5	Network pivot	Improper Access Control
CVE-2022-30333 RARLAB unRAR Directory Traversal (Zimbra)	Threat - widespread	95	Remote code execution	Improper Access Control
CVE-2022-30525 Zyxel Firewall Unauthenticated Remote Command Injection	Threat - widespread	1	Network pivot	Injection
CVE-2022-30190 "Follina" Microsoft Support Diagnostic Tool (MSDT) Arbitrary Code Execution	Threat - widespread (0 day)	0	Social engineering	Injection
CVE-2022-26134 Confluence Server and Data Center Unauthenticated Remote Code Execution (OGNL Injection)	Threat - widespread (0 day)	0	Remote code execution	Injection
CVE-2022-33891 Apache Spark Command Injection	Threat - widespread	4	Remote code execution	Injection
CVE-2022-26138 Hard-coded Password in Questions for Confluence Application for Confluence Server and Data Center	Threat - widespread	1	Remote code execution	Improper Access Control
CVE-2022-37042 Zimbra Collaboration Suite Authentication Bypass	Threat - widespread (0 day)	0	Remote code execution	Improper Access Control
CVE-2022-36804 Atlassian Bitbucket Server and Data Center Command Injection	Threat - widespread	27	Remote code execution	Injection
CVE-2022-27593 QNAP QTS Photo Station Externally Controlled Reference	Threat - widespread (0 day)	0	Network pivot	Improper Access Control

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-41352 Zimbra Collaboration Suite Remote Code Execution	Threat - widespread (0 day)	0	Remote code execution	Injection
CVE-2022-41082 "ProxyNotShell" Microsoft Exchange Server Remote Code Execution	Threat - widespread (0 day)	0	Remote code execution	Improper Access Control
CVE-2022-41040 "ProxyNotShell" Microsoft Exchange Server Server-Side Request Forgery	Threat - widespread	0	Remote code execution	Injection
CVE-2022-40684 Fortinet FortiOS Authentication Bypass	Threat - widespread (0 day)	0	Network pivot	Improper Access Control
CVE-2022-41073 Microsoft Windows Print Spooler Elevation of Privilege	Threat - widespread (0 day)	0	Local code execution	Memory Corruption
CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege "OWASSRF"	Threat - widespread	42	Remote code execution	Injection

** Exploitation in the wild privately reported to Rapid7*

For the most part, the first six weeks of 2022 were dominated by widespread exploitation of various business-critical technologies vulnerable to Log4Shell. In particular, VMware vCenter and Horizon servers saw sustained mass attacks, prompting warnings from CISA and the UK's National Health Service (NHS) in addition to security company communications about observed exploitation. Rapid7 managed services teams observed exploitation across dozens of customers in January. Attackers also targeted Ubiquiti UniFi controllers and Zyxel devices, both of which offered initial access vectors.

Unrelated to Log4Shell, CVE-2021-20038, a Rapid7-discovered buffer overflow in SonicWall SMA 100 devices, began seeing rather clumsy exploitation attempts the last week of January 2022. In defiance of barriers to scalable exploitation, CVE-2021-20038 made CISA's April 2022 list of "Routinely Exploited Vulnerabilities," landing it squarely in widespread threat territory, unpredictable as that outcome may have been. In the last few weeks of 2022, Rapid7 was also informed privately that at least one organization saw in-the-wild exploitation of CVE-2021-20038 as early as December 16, 2021, a mere nine days after SonicWall sent customers their disclosure — and three-plus weeks before Rapid7's research team published our own.

Success, or lack thereof, of exploit attempts was a recurring topic of conversation throughout 2022. Astute readers may have noticed that Spring4Shell (CVE-2022-22965) is conspicuously missing from our catalog of widespread threats, in spite of well-documented mass exploitation attempts. While the occasional web shell did make it onto a host via Spring4Shell, it's not clear that the vast majority of these exploit attempts were hitting vulnerable code paths. Similarly, the ironically named "Text4Shell" (CVE-2022-42889) — a remote code execution bug in Apache Commons Text that we refused on principle to include in our dataset at all — saw a high volume of exploit attempts within a week of disclosure, but we're still awaiting definitive confirmation that any vulnerable real-world applications were actually affected.

March, April, and May made for a blustery spring for security teams, with a widely exploited vulnerability appearing roughly once a week for the whole of the three-month period, though notably, exploitation wasn't always immediate. Remote code execution bugs in Spring Cloud Gateway (CVE-2022-22947) and Spring Cloud Function (CVE-2022-22963) rounded out a bad March for Spring

products: CVE-2022-22947 was eventually incorporated into the cryptojacking Sysrv-K botnet, per Microsoft. Matthew Remacle, a researcher at security firm GreyNoise Intelligence, privately shared data on several spikes of activity targeting Spring Cloud Function, with the highest payload count manifesting in Q2 2022; most of the payloads GreyNoise saw were indicative of low-skilled attacks (i.e., a heavy concentration of repurposed Nuclei templates).

At the end of the first week of April, VMware published an advisory warning of serious remote code execution (CVE-2022-22954) and privilege escalation (CVE-2022-22960) flaws in their Workspace ONE Access solution. On May 18, CISA issued an alert about threat actor activity that had evidently started only two days out from the original advisory. The chain would turn out to be one of the most widely used attacks of 2022: to date, the vulnerabilities have been exploited to deploy ransomware, drop coin miners, install botnet malware, and more.

May brought remote code execution vulnerabilities in F5 BIG-IP (CVE-2022-1388) and Zyxel firewalls (CVE-2022-30525), both of which were exploited to drop cryptocurrency miners and web shells within a few days. Naturally, just before Memorial Day in the U.S., the security research community discovered a novel malicious document file that had been used in the wild and was evading Windows Defender detection. The maldoc attack vector turned out to be a zero-day flaw in the Microsoft Support Diagnostic Tool (MSDT). The community nicknamed the vulnerability "Follina" before Microsoft assigned CVE-2022-30190 several days later.

Community interest in the Follina mystery may have contributed to the vuln's weirdly enduring notoriety: Despite the fact that Follina is one of many malicious attachment-type attacks used in the wild, ransomware actors seem to have picked it up, and security firm WatchGuard named it a "top security incident" in a mid-year threat report. Rapid7's own threat intel detection engineering team also noted a steady stream of Follina detections in the weeks following the vulnerability's discovery, with one big caveat — namely, that the overwhelming majority of detections were security personnel testing proofs of concept, or the occasional pen tester executing a social engineering operation.

The Follina buzz hadn't yet faded when one of 2022's defining security incidents hit, looking to steal the mass exploitation crown from earlier VMware Workspace ONE Access and F5 BIG-IP CVEs. On June 2, Australian technology company Atlassian published a security advisory for CVE-2022-26134, an actively exploited zero-day remote code execution vulnerability in on-premise instances of its hugely popular Confluence software. At the time of the advisory's publication, CVE-2022-26134 was unpatched; Atlassian released a fix on June 3, after making the (correct) decision to release vulnerability information the day prior. The Confluence vulnerability offered a classic example of “many attackers, many targets,” as ransomware groups, cryptocurrency mining campaigns, and state-sponsored threat actors leveraged CVE-2022-26134 for nefarious ends.

Other 2022 widespread threats included CVE-2022-40684, a critical authentication bypass in widely deployed Fortinet firewalls and web proxies; CVE-2022-29499, a zero-day vulnerability in Mitel MiVoice Connect appliances that provided an initial access vector for Lorenz ransomware; CVE-2022-26138, a hard-coded password vulnerability in Atlassian’s Questions for Confluence application; yet another QNAP zero-day flaw (CVE-2022-27593) used in prolific DeadBolt ransomware attacks; and a mind-boggling array of Zimbra Collaboration Suite vulnerabilities, including two zero-days (CVE-2022-37042, CVE-2022-41352) and an upstream bug in unRAR (CVE-2022-30333) that were all used to deploy web shells in the wild.

We Need to Talk About Exchange (Again)

Well, here we are again. If anyone bet a pony on 2022 offering a reprieve from widely exploited vulnerabilities in on-premises instances of Microsoft Exchange Server, they lost that bet definitively. At the end of September 2022, Vietnamese security firm GTSC published information and IOCs on what they claimed was a pair of unpatched Microsoft Exchange Server vulnerabilities being used in attacks on their customers’ environments dating back to early August. Microsoft confirmed both zero-day vulnerabilities later the same day and said they were aware of "limited, targeted attacks” using the two vulnerabilities, which were assigned CVE-2022-41040 and CVE-2022-41082.

The vulns required authenticated network access for successful exploitation and appeared to be a variant of 2021’s infamous ProxyShell attack chain (CVE-2021-34523, CVE-2021-34473, CVE-2021-31207), though notably, ProxyShell didn’t require authentication. Security researcher Kevin Beaumont christened the new zero-day chain “ProxyNotShell,” as security teams waited hopefully for a quick fix.

It didn’t come. October 2022’s Patch Tuesday came and went without a patch for the ProxyNotShell vulns, and systems administrators had to make do with a temporary mitigation—more specifically, a regular expression-based block rule that attackers quickly bypassed. Microsoft updated the rule, attackers bypassed it again, and on and on the cycle went, leaving security teams confused and frustrated.

A true fix arrived on November 8, 2022, but historically, Exchange patch uptake has been much slower than the pace of attacks. Six weeks after the patch was released, mere days before Christmas, security firm CrowdStrike published a blog disclosing a fresh exploit technique that bypassed Microsoft's suggested mitigation technique by using the Outlook Web Application (OWA) endpoint as the initial attack vector rather than the Autodiscover endpoint Microsoft's block rule had considered. CrowdStrike had discovered the new exploit while investigating several Play ransomware incidents. Rapid7 managed services teams similarly saw an uptick in incidents stemming from exploitation of unpatched Microsoft Exchange Server installations, including to deploy ransomware.

The spruced-up attack chain was nicknamed "OWASSRF." But only servers that hadn't applied the November 8 patch were vulnerable to the new technique; CrowdStrike assessed that the OWA vector probably mapped to CVE-2022-41080, which was fixed at the same time as CVE-2022-41040 (whose exploitation was the first step in the original ProxyNotShell attack chain) and CVE-2022-41082 (the secondary remote code execution step).

Even with a fresh barrage of attacks aimed at Exchange servers, tens of thousands of vulnerable systems persist on the open internet. We hear 2023 might finally be the year of the Linux desktop — maybe it'll also be a year without fresh 0day in on-prem Exchange.

Other Known Exploited Vulnerabilities

Rapid7 teams tracked a number of known-exploited vulnerabilities in 2022 that were not categorized as widespread threats, 17 of which we deemed interesting or notable. This category usually carries a little bit of intrigue, as known-exploited flaws with no evidence of widespread exploitation are, in our experience, likelier to have arisen from zero-day exploits (mystery!), and also likelier to lack in-depth details (rude!). At time of writing, two of the vulnerabilities listed below (CVE-2022-31199, CVE-2022-28810) were not on CISA's KEV list.

Table 2: 2022 exploited in the wild CVEs

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2021-35587 Oracle Access Manager Remote Code Execution	Threat - exploited in the wild	233	IT security management compromise	Deserialization
CVE-2022-24112 Apache APISIX Remote Code Execution	Threat - exploited in the wild	17	Cloud infrastructure compromise	Improper Access Control
CVE-2022-0543 Redis Lua Sandbox Escape Remote Code Execution (Debian)e	Threat - exploited in the wild	21	Remote code execution	Improper Access Control
CVE-2022-26318 WatchGuard Firebox and XTM Appliance Arbitrary Code Execution	Threat - exploited in the wild	4	Network pivot	Unknown
CVE-2022-0847 "Dirty Pipe" Linux Local Privilege Escalation	Threat - exploited in the wild	49	Local code execution	Improper Access Control
CVE-2022-26501 Veeam Backup & Replication Authentication Bypass	Threat - exploited in the wild	Unknown	IT security management compromise	Improper Access Control
CVE-2022-1040 Sophos Firewall Authentication Bypass	Threat - exploited in the wild (0day)	0	Network pivot	Improper Access Control
CVE-2022-22965 "Spring4Shell" Spring Framework WebDataBinder Remote Code Execution	Threat - exploited in the wild (0day)	0	Remote code execution	Injection
CVE-2022-28810 Zoho ManageEngine ADSelfService Plus Remote Command Injection	Threat - exploited in the wild (0day)	0	IT security management compromise	Injection
CVE-2022-26925 Microsoft Windows LSA Spoofing Vulnerability	Threat - exploited in the wild (0day)	0	IT security management compromise	Improper Access Control

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-26923 Active Directory Privilege Escalation	Threat - exploited in the wild	100	IT security management compromise	Improper Access Control
CVE-2022-35405 Zoho ManageEngine Password Manager Pro Unauthenticated Remote Code Execution	Threat - exploited in the wild	75	IT security management compromise	Deserialization
CVE-2022-31199 Netwrix Auditor Arbitrary Code Execution	Threat - exploited in the wild	30**	IT security management compromise	Deserialization
CVE-2022-40139 Trend Micro Apex One Improper Validation Vulnerability	Threat - exploited in the wild (0day)	0	IT security management compromise	Improper Access Control
CVE-2022-3236 Sophos Firewall Remote Code Execution	Threat - exploited in the wild (0day)	0	Network pivot	Injection
CVE-2022-42475 Fortinet FortiOS Heap-Based Buffer Overflow	Threat - exploited in the wild (0day)	0	Network pivot	Memory Corruption
CVE-2022-27518 Citrix ADC Arbitrary Code Execution	Threat - exploited in the wild (0day)	0	Network pivot	Improper Access Control

*** Estimated*

Of particular note are five different zero-day vulnerabilities in security gateway and firewall products, all of which seem to have been exploited before disclosure, in addition to a mysterious vuln in WatchGuard Firebox (CVE-2022-26318) that we couldn't confirm was exploited as a zero-day, and that may be linked to Cyclops Blink threat activity detailed in a February 2022 CISA alert. There's also little detail on exploits or threat actors targeting Fortinet (CVE-2022-42475) and Trend Micro Apex One (CVE-2022-40139), though this was one of at least two Apex One zero-day vulnerabilities that debuted in 2022.

More is known about CVE-2022-27518 thanks to a December 2022 U.S. National Security Agency (NSA) bulletin on APT5 activity targeting Citrix ADC installations. CVE-2022-27518 isn't mentioned explicitly, but the document contains a link to Citrix's advisory, which was published the same day as the NSA warning. Rapid7 has also kept an eye on Citrix ADC as a perennially popular target for both skilled and commodity attackers.

Rounding out the security gateway entries are CVE-2022-3236 and CVE-2022-1040, two remote code execution vulnerabilities in Sophos Firewalls that were exploited in targeted attacks against South Asian customers, as indicated in disclosures released six months apart. Initially we didn't pay much attention to these, as Sophos Firewalls auto-update by default (yay!), which should mean less opportunity for many attackers to exploit the vulns. But the number of advanced threat actors using CVE-2022-1040 is, frankly, compelling: The flaw has been linked to APT operations targeting Ukraine, Tibetans, and South Asian victims in Afghanistan, Bhutan, India, Nepal, Pakistan, and Sri Lanka. CVE-2022-3236 doesn't yet have a similarly long list of exploit targets, but it's not a stretch to imagine it was (or will be) used in similar operations as long as there's unpatched attack surface area.

Microsoft Active Directory attack techniques had a big(ger) year in 2021 following a SpecterOps presentation at Black Hat USA outlining a dozen-plus new techniques for abusing Active Directory Certificate Services (AD CS). In May 2022, researcher Oliver Lyak at the Danish Institute for Cyber Risk (IFCR) detailed a new technique that leveraged a weakness in AD CS certificate templates to escalate privileges. Nicknamed "Certifried," the issue was tracked as CVE-2022-26923 and patched in Microsoft's May 2022 Patch Tuesday release; however, as several sources pointed out, AD administrators needed to take additional action post-patch since not all attack avenues were fully remediated. CISA added CVE-2022-26923 to their Known Exploited Vulnerabilities (KEV) list on August 18, 2022 without additional context.

The first mention of CVE-2022-31199, a code execution bug in Netwrix Auditor IT software that was disclosed in July 2022, was a December 2022 threat brief describing a spike in TrueBot malware infections that went back to August 2022. The software in question wasn't found to have a large internet-facing footprint, but the original Bishop Fox advisory describing the flaw emphasizes that the vulnerable service is frequently executed with high privileges in an Active Directory environment, opening an avenue for AD compromise.

Veeam CVE-2022-26501 (along with CVE-2022-26500) was cited in a December 2022 analysis from Kroll on novel tactics observed in AvosLocker ransomware incidents. Veeam's backup solution was abused to exfiltrate data before the threat actor deleted backups; earlier in the year, Veeam was also abused for credential stealing in connection with various ransomware crews, though specific CVEs weren't mentioned.

Apache APISIX CVE-2022-24112, a remote code execution vulnerability disclosed in February 2022, appeared on CISA's list of CVEs routinely exploited by Chinese state-sponsored actors, alongside previously mentioned vulns in F5 (CVE-2022-1388) and Atlassian (CVE-2022-26134) software.

Spotlight: ManageEngine Zero-Day Detected in the Wild (CVE-2022-28810)

In April 2022, Rapid7 managed services teams detected unusual activity across multiple customer environments. The activity turned out to be a financially motivated campaign conducted by a skilled threat actor. In almost all cases, the adversary used default administrative credentials to gain access to publicly facing instances of Zoho ManageEngine ADSelfService Plus and Desktop Central before abusing the custom scripts feature in ADSelfService Plus.

The Rapid7 vulnerability research team developed an exploit that replicated the attacker behavior and determined that there was a zero-day vulnerability in ADSelfService Plus. The vulnerability arose from a feature that allowed the admin user to execute arbitrary operating system commands after a password reset or account lockout status update; it was trivial for a threat actor with stolen or default admin credentials to execute operating system (OS) commands remotely on the target system to achieve persistence and pivot further into the environment. Moreover, because the %password% variable in scripts wasn't sanitized or obfuscated, the admin user could observe all password changes, potentially allowing them to recover valid credentials for Active Directory accounts.

Rapid7 reported the security issues to Zoho, who fixed the security issues by making several changes, including no longer accepting scripts through the web interface and requiring post action scripts to be placed on disk by a user with access to the underlying operating system. CVE-2022-28810 was assigned as an umbrella for the various issues reported and fixed. In November 2022, an ESET research report detailing advanced persistent threat (APT) activity noted that CVE-2022-28810 was the suspected culprit in the compromise of a U.S. defense contractor's ADSelfService Plus instance.

The full vulnerability disclosure for CVE-2022-28810 is here.

Impending Threats

Once again this year, our impending threats list has dwindled in order to make room for the many vulnerabilities that have seen active or mass exploitation. While we could easily leave impending threats out of our vulnerability dataset entirely, we believe this is an important category, particularly when it highlights products or flaws that are more likely to escape scrutiny or exploit detection.

Table 3: 2022 impending threat CVEs

CVE	Threat Status	Disclosure Date	Attacker Utility	Vulnerability Class
CVE-2022-37393 Zimbra Collaboration Suite Root Privilege Escalation	Impending threat - exploit available	10/27/2021	Local code execution	Improper Access Control
CVE-2022-28219 Zoho ManageEngine ADAudit Plus Remote Code Execution	Impending threat - exploit available	3/30/2022	IT security management compromise	Injection
CVE-2022-20829 Cisco ASDM Arbitrary Code Execution via Lack of Package Signing	Impending - tooling available	06/22/2022	IT security management compromise	Improper Access Control
CVE-2022-2992 GitLab CE/EE Remote Command Execution	Impending - exploit available	10/06/2022	Remote code execution	Injection
CVE-2021-39144 VMware Cloud Foundation (NSX-V) XStream Remote Code Execution	Impending - exploit available	10/25/2022	Cloud infrastructure compromise	Deserialization

Products made by the vendors listed above have been targeted frequently, in no small part because of their large deployment footprints. We haven't been able to definitively confirm exploitation of Zimbra Collaboration Suite CVE-2022-37393, which went unpatched for nearly a year, but with widespread exploitation of many other Zimbra flaws, it's hardly a stretch to assume attackers would be tempted to leverage a privilege escalation that delivered root privileges. Likewise, a variety of Zoho ManageEngine software has been broadly exploited the past few years, and while ADAuditPlus seems to have a small internet-facing target population, multiple public exploits are available for CVE-2022-28219.

In August 2022, at Black Hat USA and DEF CON 30, Rapid7 disclosed 10 different security issues affecting Cisco Adaptive Security Software (ASA), Adaptive Security Device Manager (ASDM), and FirePOWER Services Software for ASA. Among these issues was CVE-2022-20829, which highlighted a lack of any type of cryptographic signature to verify the Cisco ASDM package's authenticity. Researcher Jake Baines discovered that it was possible to modify the contents of an ASDM package, update a hash in the package's header, and successfully install the package on a Cisco ASA — meaning an attacker could craft an ASDM package that contains malicious installers, malicious web pages, and/or malicious Java. An administrator using the ASDM client could then connect to the ASA and download or execute attacker-provided Java, giving the attacker access to the administrator's system.

This isn't an attack that's likely to propagate among low-skilled adversaries, but it's exactly the type of attack that sophisticated threat actors would use — and have used in the past. A malicious ASDM package could be installed in a supply chain attack, leveraged by an insider threat, installed by a third-party vendor/administrator, or made available "for free" on the internet for administrators to discover themselves (as those without valid Cisco contracts might be tempted to do). As part of the vulnerability disclosure, Rapid7 published a tool that demonstrates extracting and rebuilding "valid" ASDM packages. It can also generate ASDM packages with an embedded reverse shell.

Rounding out our impending threats category this year are CVE-2022-2992, an authenticated remote code execution vulnerability in GitLab software, and CVE-2021-39144, an unauthenticated remote code execution vuln in VMware Cloud Foundation's implementation of XStream, an open-source XML serialization library. Successful exploitation of CVE-2021-39144 offers malicious actors code execution as root on NSX-V appliances thanks to an unauthenticated endpoint that leverages XStream for input serialization. Public exploits are available for both vulnerabilities.

2020 and 2021 Impending Threats: Where Are They Now?

While this report focuses on vulnerabilities that were exploited or otherwise significant in 2022, it's essential to note that older vulnerabilities continue to be exploited widely and should also be prioritized for remediation. In CISA's list of routinely exploited vulnerabilities from 2021, more than a quarter of the highlighted CVEs were from 2020 or earlier — meaning there were enough of those unpatched systems that exploiting vulnerabilities a year old (or two, or three, or four years old) was still a reliable option for attackers.

In that same vein, we've watched impending threats from our 2020 and 2021 Vulnerability Intelligence reports slowly make their way into threat intelligence briefs and news articles, even multiple years later. 44% of the CVEs Rapid7 classified as impending threats in previous intelligence reports have been exploited in the wild as of December 2022, up from 25% at the end of 2021. At least five impending threats from past years have been exploited at scale by ransomware groups, cryptocurrency mining operations, or botnet malware:

CVE-2020-0609: Windows Remote Desktop Gateway Remote Code Execution "BlueGate"

CVE-2020-5135: SonicWall SonicOS Portal Buffer Overflow

CVE-2020-2021: Palo Alto Networks PAN-OS SAML Authentication Bypass and Remote Code Execution

CVE-2020-16846: SaltStack Salt Command Injection

CVE-2021-34481: Microsoft Windows Print Spooler Remote Code Execution

Rapid7's 2021 Vulnerability Intelligence Report also emphasized the risk of "Bring Your Own Vulnerable Driver (BYOVD)" attacks, where an adversary with administrative privileges installs a legitimately signed driver with known vulnerabilities on the victim system. BYOVD attacks have been commonly used in the wild, as Rapid7 researchers detailed in depth in December 2021. But even though this style of attack has demonstrable uptake among adversaries, we've also seen that product security incident response teams (PSIRTs) tend to lose interest when evaluating BYOVD vulnerability disclosures, because administrator-level privileges are required from the start.

As it happens, BYOVD attacks surged in 2022: Multiple security firms reported in-the-wild exploitation of vulnerable drivers, threat reports were dedicated to analyzing driver-based attacks, and media coverage underscored BYOVD adoption by ransomware groups. As we noted in the list above, CVE-2021-34481, which allows non-administrative users to add arbitrary signed drivers to the Windows Driver Store, has also been linked to ransomware usage, though sources seem to incorrectly categorize it as a PrintNightmare variant rather than consider it a driver-based vector.

Organizations looking to protect themselves from some driver-based attacks can employ Microsoft's driver block rules, which should in theory prevent known-bad drivers from being loaded — if Redmond actually fixed the update mechanism that puts those rules into action following community feedback that bad drivers weren't being blocked as advertised.

Notable Attack Trends

Time to Known Exploitation

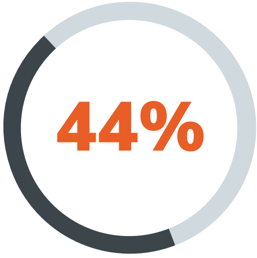
As a key metric, Rapid7 researchers track the time between when vulnerabilities become known to the public and when they are reported as exploited in the wild. This window, which we call "Time to Known Exploitation" (TTKE), gives organizations a sense of how quickly significant vulnerabilities are incorporated into attacker arsenals after they're released in advisories or threat briefs (or on social media). As usual, we're not trying to capture the full volume of zero-day exploitation in the wild, a not-insignificant amount of which spans browser- and host-based vulnerabilities, which we traditionally exclude except for extraordinary cases.

We take a generally conservative approach to defining TTKE. In most cases, the values for time to known exploitation mean that **at most**, each vulnerability was exploited within the number of days specified. If we take CVE-2021-4034, for instance, the "153" is based on the date the vulnerability was added to CISA's Known Exploited Vulnerabilities (KEV) list, which almost certainly was not the first time it was exploited in the wild.

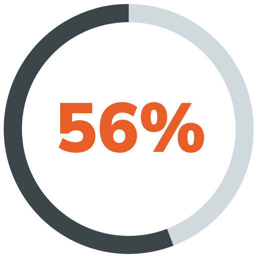
We've also estimated TTKE in a few cases — for example, when a third-party incident response report specifies that a CVE was exploited during a particular month but doesn't specify the day exploitation was first detected (e.g., "in early August"), we take a conservative approach and use the middle or later part of that timeline as our TTKE value. For the most part, a margin of error of a few weeks is acceptable. If the margin of error could reasonably be months (e.g., CVE-2022-26352), we list TTKE as "Unknown."

First, the good news: **Average** time to known exploitation for our 2022 vulnerabilities was 24.5 days — more than twice as long as 2021's meager average TTKE of 12 days.

Now, the bad news: Averages are fickle creatures, and higher TTKE values for certain 2022 vulnerabilities obscures the litany of zeroes attached to a big swath of others. 56% of the vulnerabilities in this report were exploited within seven days of public disclosure—a 12% rise over 2021 and an 87% rise over 2020. If we look at the **median** value instead of taking the average, median time to exploitation in 2022 was **one day** across the vulnerabilities we've included in this report. (To be fair, the median time to exploitation in 2021 was zero, so we can hold on to a single-day improvement as a faint silver lining.)



exploited vulnerabilities arose from a zero-day exploit



of the vulnerabilities were exploited within seven days of public disclosure

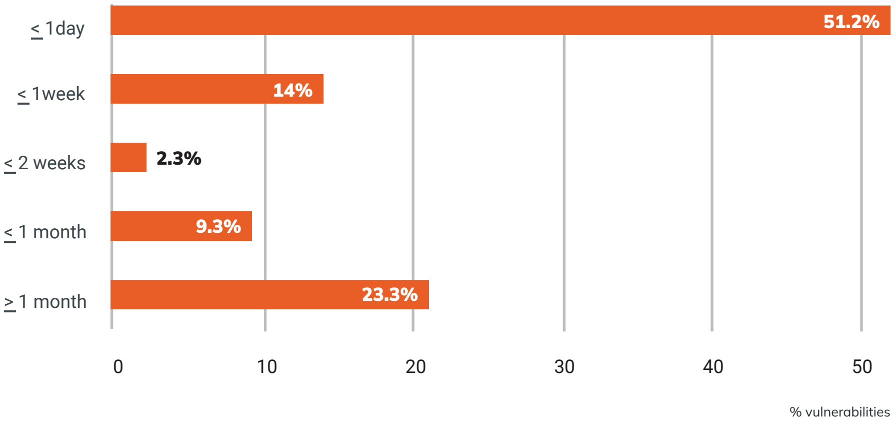
87%

rise over 2020

12%

rise over 2021

Time to Known Exploitation (TTKE/days)



Over the past two years, a flood of zero-day exploits seems to have become the new normal. 44% of known exploited vulnerabilities in this report arose from a zero-day exploit, though the occasional data validation challenge could reasonably skew that by a few percentage points. Some of the challenge in determining TTKE hangs on the definition of "public" or "disclosed" — for example, the change that remediated CVE-2022-22963 in Spring Cloud Function was committed in a public GitHub repository on March 24, 2022, without any mention of a CVE or a security issue. Akamai began observing exploitation in the wild on March 27, two days before the fixed version of Spring Cloud Function was officially released with a CVE on March 29. We chose to use "0" as our TTKE value for CVE-2022-22963, since it's unreasonable to expect the general public (including Spring Cloud customers) to examine individual GitHub commits for potential security implications.

CVE-2022-42475, a heap-based buffer overflow vulnerability in Fortinet's FortiOS, makes for a similar edge case — and here's where the "coordinated" part of coordinated vulnerability disclosure is important. On December 9, 2022, a French security company published a bulletin on a critical, non-public vulnerability in Fortinet SSL VPNs. As it turned out, Fortinet had privately given customers early warning about the vulnerability the week of December 7, but didn't release a public advisory until December 12. When the advisory was published, it included a note that Fortinet was "aware of an instance where this vulnerability was exploited in the wild," but failed to specify whether the flaw had been exploited by threat actors before they released a fixed version — which they evidently did silently on November 28, 2022, potentially giving adversaries time to reverse engineer the patch and develop exploits before customers knew there was even a remediation to implement.

Was CVE-2022-42475 true zero-day exploitation? Probably, given the vulnerability's root cause and the circumstances. Timelines are tricky, as anyone who's had to compile a good one knows. But the true harm of silent patches isn't our inability to definitively express a TTKE value; it's that they ensure only skilled adversaries get a head start — and they don't need it.

Any way you skin it, attackers are fast, and general consensus is that they've grown increasingly efficient at targeting vulnerabilities both new and known in the wild. In order to develop policies and practices that mitigate the risk of faster time to exploitation, security practitioners need not only detailed guidance, but also the "why" behind it — and that means vulnerability details, delivered transparently, in ways accessible to security teams and researchers. To intentionally obfuscate these details from customers, security solution vendors, and academics only cedes the initiative to the attackers who already are demonstrably skilled at reversing under-documented patches.

Ransomware

By all accounts, the ransomware ecosystem continued to mature and expand in 2022, as multiple newcomers established operations and news broke of high-profile attacks on world governments, intelligence agencies, municipal systems, school districts, critical infrastructure, and — of course — private businesses spanning every possible vertical.

The island nation of Vanuatu was knocked completely offline for more than a month after a ransomware attack felled its IT systems in November 2022, causing the Australian government to step in to assist. Costa Rica declared a state of emergency in April 2022 after being subjected to weeks of ongoing attacks. In May, the U.S. State Department called Conti ransomware "the costliest strain of ransomware ever documented" and offered millions of dollars in rewards for information that would help bring Conti ransomware threat actors to justice (which may or may not have succeeded).

Table 4: 2022 ransomware CVEs

CVE	Threat Status	TTKE in Days	Ransomware Attack?	Attacker Utility	Vulnerability Class
CVE-2022-41073 Microsoft Windows Print Spooler Elevation of Privilege	Threat - widespread (0day)	0	Yes	Local code execution	Memory Corruption
CVE-2022-21882 Microsoft Windows Win32k Elevation of Privilege	Threat - widespread (0day)	0	Yes	Local code execution	Memory Corruption
CVE-2022-26134 Confluence Server and Data Center Unauthenticated Remote Code Execution (OGNL Injection)	Threat - widespread (0day)	0	Yes	Remote code execution	Injection
CVE-2022-30190 "Follina" Microsoft Support Diagnostic Tool (MSDT) Arbitrary Code Execution	Threat - widespread (0day)	0	Yes	Social engineering	Injection
CVE-2022-29499 Mitel MiVoice Connect Service Appliance Data Validation Vulnerability	Threat - widespread (0day)	0	Yes	Network pivot	Injection
CVE-2022-27593 QNAP QTS Photo Station Externally Controlled Reference	Threat - widespread (0day)	0	Yes	Network pivot	Improper Access Control
CVE-2022-41082 "ProxyNotShell" Microsoft Exchange Server Remote Code Execution	Threat - widespread (0day)	0	Yes	Remote code execution	Improper Access Control

CVE	Threat Status	TTKE in Days	Ransomware Attack?	Attacker Utility	Vulnerability Class
CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege "OWASSRF"	Threat - widespread	42	Yes	Remote code execution	Injection
CVE-2021-44228 Log4Shell Remote Code Execution in VMware vCenter Server and VMware Horizon	Threat - widespread	26	Yes	Remote code execution	Injection
CVE-2022-22954 VMware Workspace ONE Access / Identity Manager Remote Code Execution	Threat - widespread	2	Yes	Cloud infrastructure compromise	Injection
CVE-2022-22960 VMware Workspace ONE Access/Identity Manager Local Privilege Escalation	Threat - widespread	2	Yes	Local code execution	Improper Access Control
CVE-2022-26352 dotCMS Directory Traversal Remote Code Execution	Threat - widespread	Unknown	Yes	Remote code execution	Improper Access Control
CVE-2022-31199 Netwrix Auditor Arbitrary Code Execution	Threat - exploited in the wild	30**	Yes	IT security management	Deseriallization
CVE-2022-26501 Veeam Backup & Replication Authentication Bypass	Threat - exploited in the wild	Unknown	Yes	IT security management compromise	Improper Access Control

*** Estimated*

It seems like a foregone conclusion that there should be clear-cut statistics proving there were more ransomware incidents and related artifacts, including associated CVEs, in 2022 than in previous years — but strangely, that's not the case.

Only 14 of the CVEs in our 2022 vulnerability dataset could be definitively confirmed as having been used in ransomware attacks. Ransomware-mapped vulnerabilities decreased 33% year over year in 2022, in spite of the demonstrably flourishing ransomware ecosystem. That's unsettling, even if it sounds like good news.

We aren't alone in seeing ransomware-related numbers that were lower than expected. Digital Shadows noted a decline in ransomware victims in Q3 2022, cyber insurance company Coalition said ransomware claims from policyholders declined in the first half of 2022, and an annual review released by Cisco's Talos team in December 2022 shows that ransomware comprised 21% of the company's incident response (IR) engagements in 2022, compared with 38% of all IRs in 2021.

Security firm Emsisoft published a blog in January 2023 indicating that the number of ransomware incidents they saw in 2022 were "very similar" to previous years, acknowledging the difficulty of getting accurate statistical data on cybersecurity incidents. Rapid7's own managed services teams also observed ransomware incident response numbers that didn't quite meet expectations: While there were more ransomware-related incident responses overall in 2022 than in 2021, the number of ransomware incidents was lower than expected when accounting for customer growth and expected threat volume.

What could explain why ransomware numbers — imperfect and fractured though they may be — were lower than predicted in 2022? For one thing, we can't discount the possibility that some ransomware victims simply aren't reporting incidents. Like any ecosystem, however, the ransomware market is complex and interconnected, and it's likely that several factors come into play.

One potential factor that the NSA believes is influencing ransomware numbers is the sanctions stemming from the war in Ukraine, as NSA cybersecurity director Rob Joyce remarked at a UK National Cyber Security Centre (NCSC) event in May 2022:

> **"One interesting trend we see is in the last month or two ransomware is actually down. There's probably a lot of different reasons why that is but I think one impact is the fallout of Russia-Ukraine.**
>
> **As we do sanctions and it's harder to move money and it's harder to buy infrastructure in the West, we're seeing them be less effective. That is one of the knock-on effects.**

It's also possible, as a Ukrainian security firm told The Economist in November 2022, that some ransomware threat actors were pulled into the conflict, shifting the focus of their cybercrime operations away from the mass market. Even early on in the conflict there were signs of infighting among ransomware threat actors, with Lockbit going so far as to explicitly declare its neutrality. As a Reuters analysis pointed out, this move was practical, since declaring a political affiliation could undermine ransomware groups' ability to get paid — for instance, because of cyber-insurance provider loopholes that could exempt insurance payouts in cases of war.

Some responsibility for lower ransomware figures almost certainly lies with the sheer number of ransomware groups and strains that have appeared in the market, as diversification inevitably leads to changes in operations. A Q1 2022 Cisco Talos report observed that "No one ransomware family was observed twice in incidents that closed out this quarter." Rapid7 IR consultants likewise observed a vast array of ransomware families in 2022 incidents, and while global security firms tend to stay closely on top of evolving ransomware tactics, techniques, and procedures (TTPs), ransomware diversification also means more indicators and techniques to document and attribute, which takes time and expertise.

One particular trend that's picked up steam in 2022 is the buying and selling of initial access on dark web marketplaces by initial access brokers (IABs).

Initial access brokers aim to do only one thing: gain initial access. Once that access is established — either through exploitation or through means like phishing, credential stuffing, or brute force attacks — access brokers will list their targets on the dark web to sell these footholds to other cybercriminals. In essence, this decouples the attack chain and builds in latency between the initial exploitation of a vulnerable service and the follow-on actions threat analysts typically look for.

> **Initial access brokers provide a valuable service to cybercriminals like ransomware actors, since oftentimes, these cybercriminals are opportunistic about their targets.**

For defenders, this adds complexity to investigating an incident, as the chain of actions one would normally look for is often going to “start” after initial access has been established. This increases the uncertainty about when, where, and how access was gained.

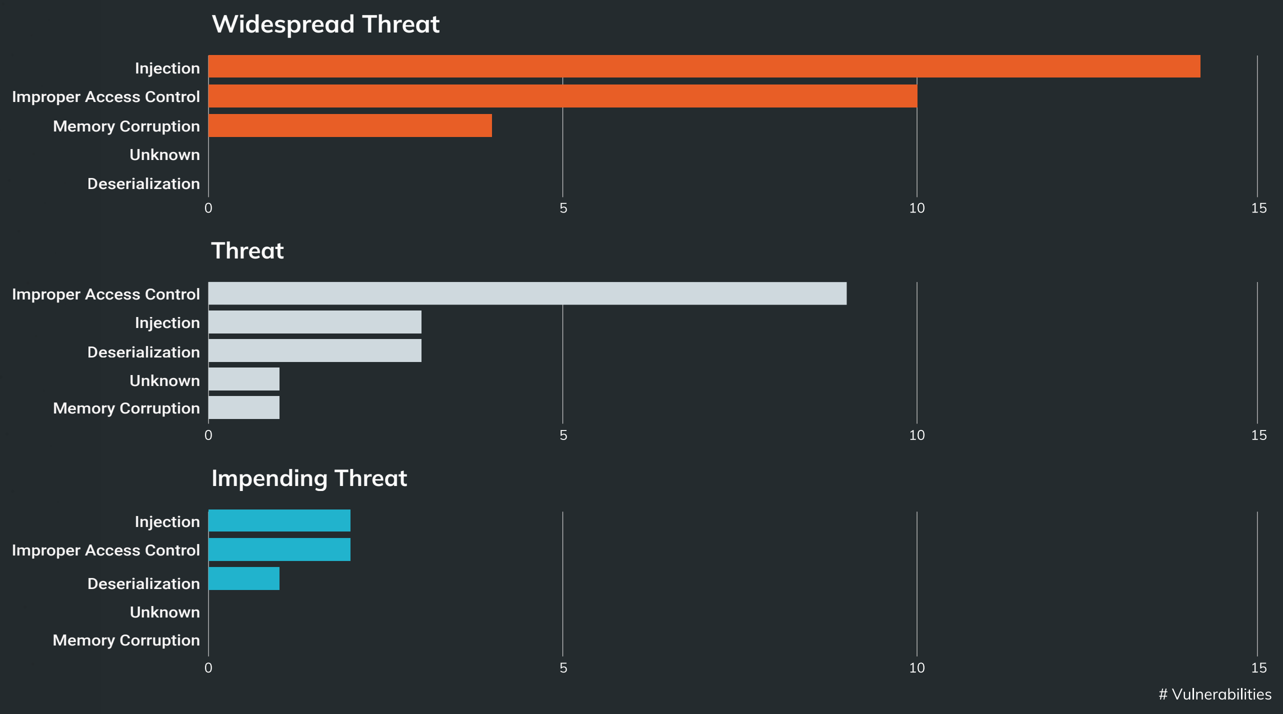
In some cases, like CVE-2022-26134, the sale is a target list. In most cases, however, the sale is access to a particular organization. The Rapid7 IntSights team has observed dark web activity where exploits were bought and sold for a number of the widely exploited vulnerabilities in this report; participants on the relevant threads are known access brokers. Even when a specific CVE isn’t mentioned, we can occasionally make conjectures about the exploit. For example, when our threat intelligence team saw an access broker post “access is via Citrix” on December 9, 2022, it’s a reasonable guess that the broker leveraged either CVE-2022-27518 or CVE-2022-27510.

Attacker Utilities and Vulnerability Classes

When getting to know a new vulnerability, the first thing our research teams look for is an understanding of the root cause and what an attacker might use that bug to achieve. Vulnerabilities arise from hundreds of conditions spanning all layers of the stack — from application programming errors to cryptographic implementations to hardware bugs. Likewise, the potential impact of any given vulnerability can vary widely based on implementation, security controls, and the sensitivity of the data or permissions an attacker can obtain as a result of exploitation.

We include two additional types of metadata in our vulnerability dataset in addition to threat status and time to known exploitation. The first piece of metadata our researchers define when analyzing emergent threats is **vulnerability class**, which is useful for making initial assessments about relative exploitability and available tooling. Deserialization flaws, for instance, come with a reputation for high exploitability and have readily available public tooling. Memory corruption vulns make frequent appearances in attacks by state-sponsored threat actors, as they often require high skill on part of exploit developers, and are less likely to be automated than something like a simple command injection exploit.

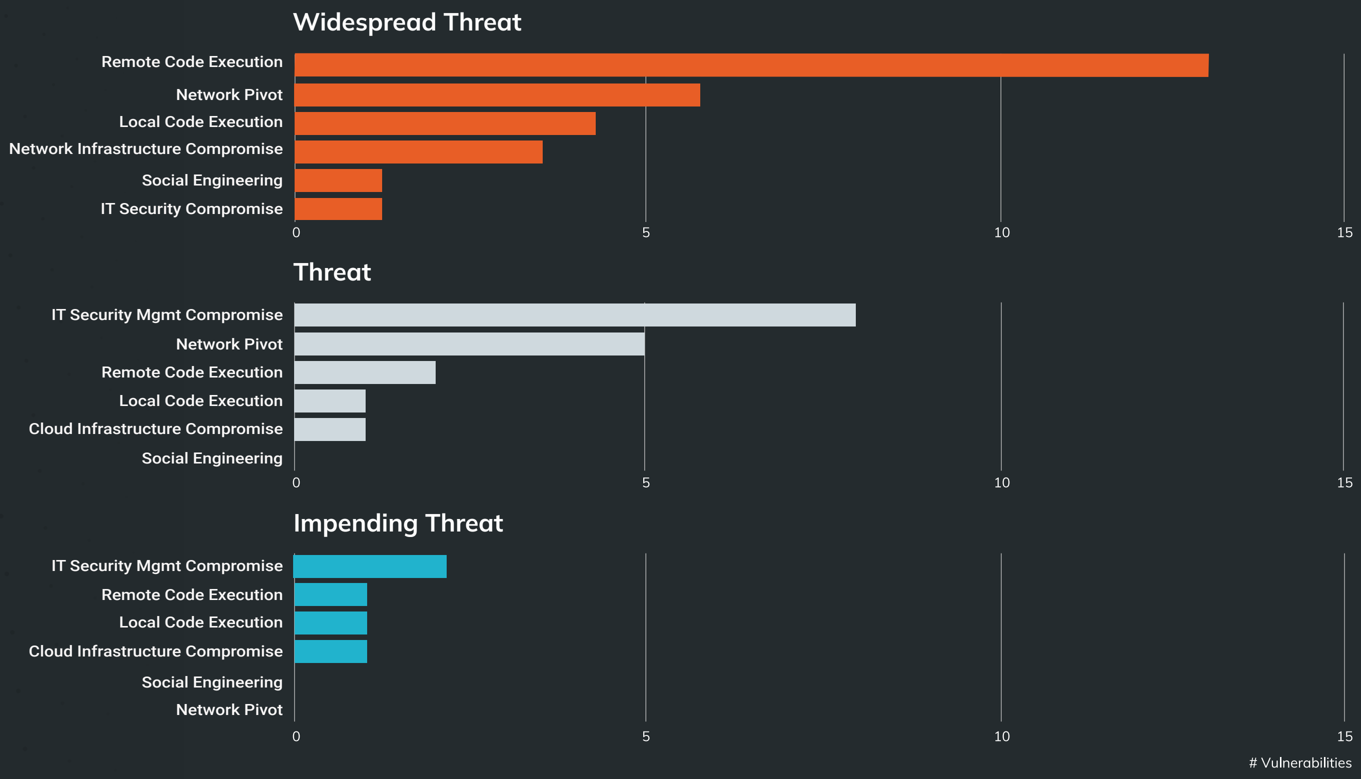
2022 Vulnerabilities by Class and Threat Status



2022 saw a slight decline in improper access control vulnerabilities (e.g., authentication bypasses) and deserialization flaws, including those exploited en masse. While memory corruptions (e.g., heap- or stack-based buffer overflows, use-after-frees) are still less represented than other categories, the number of widespread threats arising from a memory corruption flaw doubled over 2021. Finally, the injection star continued to rise: Injection attacks use specially crafted input and techniques (e.g., command injection, OGNL injection, server-side request forgery) to compromise data integrity or run arbitrary code as a high-privileged user. These attacks tend to be stable and reliable, which can make them less likely to knock over systems than some other types of exploits.

The second type of metadata we consider is **attacker utility**, which describes what an attacker can hope to gain as a result of successful exploitation — this sometimes maps to part of an exploit chain. A network pivot, for example, is an attack that gives an external adversary internal network access, while more generalized remote code execution allows an attacker to execute a payload remotely on a target.

2022 Vulnerabilities by Attacker Utility and Threat Status



In previous years, we used the term "network infrastructure compromise" as an umbrella term for vulnerabilities that led to remote code execution or takeover of things like network management, virtualization, or backup systems, which when compromised could give an attacker access to everything managed by that software or device. Our 2022 data, however, spanned so many different vulnerabilities in IT and security management solutions (e.g., access and identity management, Active Directory management) that we broke them out into a separate category. The other newcomer is cloud infrastructure compromise, which encompasses cloud gateway, API management, or other devops-related technology. We expect this category to continue to grow in threat prevalence as cloud adoption increases.

Widespread exploitation of remote code execution vulnerabilities has remained relatively consistent across our dataset year over year, as expected given this report's focus on widespread exploitation of server-side targets. Similarly, it's a no-brainer that network pivots (e.g., Fortinet CVE-2022-40684, SonicWall CVE-2021-20038) will continue to be high-value targets for both advanced and commodity attackers. "Follina" CVE-2022-30190 is the sole entry in the social engineering category, which we don't anticipate being a regular participant in these attacker utility round-ups (again, given this report's slant toward server-side bugs).

In a bit of a departure from previous years, 2022 featured four local privilege escalations that were widely exploited across VMware (CVE-2022-22960), Linux (CVE-2021-4034, aka "Pwnkit"), and Windows (CVE-2022-21882, CVE-2022-41073) environments. Privilege escalation is an indispensable part of most attack chains, but LPE tends to be underrepresented in these types of charts, particularly among widespread threats.

Spotlight: Privilege Escalation from the Perimeter

Many of the CVEs treated individually in this report can be (and have been) used in concert with one or more additional vulnerabilities to achieve something beyond the scope of a single CVE's impact. After gaining access with a remote exploit, attackers frequently need to escalate their privileges in order to achieve their objectives. They use local privilege escalation vulnerabilities to do this, yet many LPEs miss out on the spotlight (not to mention patching and detection prioritization) compared to their flashier counterparts.

Rapid7 researchers disclosed a number of local privilege escalation vulnerabilities in 2022 that exemplify this use case. CVE-2022-30526, for instance, allows a low-privileged user (e.g., nobody) to escalate to root on affected Zyxel firewalls. The vulnerability requires existing shell access to the firewall—a conundrum, until a bug like CVE-2022-30525 comes along to offer arbitrary code execution. In this particular case, not only does the vulnerable system sit on the network perimeter, the LPE was patched more than two months after the unauthenticated remote command injection vulnerability, giving savvy attackers an opportunity to find the LPE avenue on devices that had been compromised or were left unpatched after CVE-2022-30525 was disclosed.

In August of 2022, Rapid7 disclosed two local privilege escalation vulnerabilities in VMware Workspace ONE Access, Identity Manager, and vRealize Automation software. CVE-2022-31660 and CVE-2022-31661 allow an under-privileged horizon user to escalate permissions to root. Since the horizon user runs the externally accessible web application remote code execution within that component could be chained with either privilege escalation to execute code as the root user. CVE-2022-22954, the critical remote code execution vulnerability disclosed in April 2022 and widely exploited within days, provided the requisite remote access on vulnerable VMware Workspace ONE Access and Identity Manager instances.

In November 2022, Rapid7 disclosed a number of security issues in F5 BIG-IP and BIG-IQ, only two of which were assigned CVEs. One of the CVE-less issues was a local privilege escalation via bad UNIX socket permissions: F5 uses a proprietary database called mcp, which is used for persistent storage on Big-IP and related devices. The database is owned by root and accessed via a UNIX domain socket with 0777 permissions (accessible by all local users) and no authentication. Using that socket, any user on the host can add a new administrative user, granting themselves root access.

F5 declined to categorize this issue as a vulnerability, because by design, all users that log in are already `root` (and it's true that the overwhelming amount of Big-IP's attack surface runs as root already). However, several network services — including Apache Tomcat and Bind — listen on network ports and link to custom modules written in C/C++. If a vulnerability is discovered in any of those non-root services, a privilege escalation exploit path directly to root removes the small amount of privilege separation that exists.

Network edge and access control systems aren't the only example of this trend. In October of 2021, independent researcher Darren Martyn published an exploit for a zero-day root privilege escalation vulnerability in Zimbra Collaboration Suite. When successfully exploited, the vulnerability allowed a user with a shell account as the `zimbra` user to escalate to `root`. While this issue requires a local account on the Zimbra host, a slew of actively exploited vulnerabilities provide plenty of opportunity to obtain it, as we saw throughout 2022.

Defenders can get ahead of future attacks by taking care not to treat individual vulnerabilities as if they existed in a vacuum, but instead choosing to implement controls and detection mechanisms across the whole of their environment.

CONCLUSION

At Rapid7, we believe that research-driven context on vulnerabilities and emergent threats is critical to building forward-looking security programs and advancing community knowledge. Security and IT teams face mounting challenges in a heightened threat climate, and we are committed to partnering with those teams to foster better understanding of defense-in-depth strategies that will strengthen organizations' security posture, both now and in the future.

Basic vulnerability management is critical to your security program. The window for effective patching has decreased over the past three years. It is essential that organizations have emergency patching procedures and incident response playbooks in place in addition to a clearly defined, regular patch cycle that prioritizes actively and widely exploited CVEs. Without an understood, standardized mechanism for driving aligned emergency action, you're at higher risk from these increasingly frequent events.

In addition to regular and emergency patching procedures, organizations should ensure they keep current with operating system-level updates, such as Microsoft's Cumulative Updates for Windows systems. Failing to ensure timely installation of Cumulative Updates may mean that you are unable to quickly install out-of-band security patches when sudden attacks occur.

The same principle applies to all operating system-level patches, no matter the platform; OS-level vulnerabilities are a boon to attackers, even if they are not exposed to the internet.

Network edge devices (network pivots) continue to be popular and frequently exposed attack surface area. The same goes for IT or security management solutions that run with elevated privileges, as well as email servers like Microsoft Exchange. These categories of software and firmware should adhere to a zero-day patch cycle wherever possible, meaning that updates and/or downtime should be scheduled as soon as new critical advisories are released.

Limit and monitor your internet-facing attack surface area.
Understanding attack surface area and critical network entry points saves time when severe vulnerabilities surface in internet-facing technologies. Exploitation of many of the CVEs in this report — including some of those exploited in zero-day attacks — can be slowed down by limiting internet exposure of critical applications and management interfaces. Pay particular attention to security gateway products such as VPNs and firewalls, as well as anything else that's exposed by common practice or necessity.

Management and administrative interfaces should never be exposed to the public internet. The same goes for domain controllers and any other assets that organizations would not want an external attacker to be able to probe, such as IoT devices unwittingly exposed online. Audit internet-exposed attack surface area regularly, including via external penetration tests, if possible.

Ensuring that (preferably aggregated) logging is set up across networks and hosts will save some time during active threat events. There are several community-driven signature repositories and low-cost rulesets that can give defenders at least basic visibility into potential intrusions in their environments, along with a plethora of commercial solutions. Knowing ahead of time what kind of visibility you have into suspicious events will drive faster and more effective responses during critical situations.

Future Rapid7 Research

Rapid7 researchers and community members publish analysis of high-priority vulnerabilities in Rapid7's open vulnerability assessment platform, AttackerKB. These analyses often include sample proof-of-concept code and indicators of compromise in addition to exploitation timelines and attack chain analysis. To contribute or subscribe to Rapid7 notifications in AttackerKB, create a free account here.

New Rapid7 zero-day vulnerability research is often published here.

When a new threat arises, Rapid7 guidance can be found in the emergent threats section of the Rapid7 blog, along with corresponding information for Rapid7 product and services customers. If you are a customer, we'd love to hear your feedback on this report. You can contact your CSM or TAM, or contact us at research@rapid7.com.

Appendix

This dataset does not include all CVEs or even all active threats we evaluated in 2022, but it does represent a diverse sample of attacker use cases and exploitation case studies, with heavy emphasis on widespread attacks. Our intent is not to imply that any one CVE or vulnerability group is less important than others. Security teams, network administrators, and defenders at large have in-depth understanding of which assets are critical in their environments and how action taken may affect their business priorities. What we offer is an attacker-centric view of the vulnerability landscape that Rapid7 customers and the security community can use to inform the policies and practices that they employ as part of a larger defense-in-depth strategy.

Full 2022 Dataset

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-40684 Fortinet FortiOS Authentication Bypass	Threat - widespread (0 day)	0	Network pivot	Improper Access Control
CVE-2022-41352 Zimbra Collaboration Suite Remote Code Execution	Threat - widespread (0 day)	0	Remote code execution	Injection
CVE-2022-41073 Microsoft Windows Print Spooler Elevation of Privilege	Threat - widespread (0 day)	0	Network pivot	Improper Access Control
CVE-2022-21882 Microsoft Windows Win32k Elevation of Privilege	Threat - widespread (0day)	0	Local code execution	Memory Corruption
CVE-2022-26134 Confluence Server and Data Center Unauthenticated Remote Code Execution (OGNL Injection)	Threat - widespread (0day)	0	Remote code execution	Injection
CVE-2022-30190 "Follina" Microsoft Support Diagnostic Tool (MSDT) Arbitrary Code Execution	Threat - widespread (0day)	0	Social engineering	Injection
CVE-2022-29499 Mitel MiVoice Connect Service Appliance Data Validation Vulnerability	Threat - widespread (0day)	0	Network pivot	Injection

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-37042 Zimbra Collaboration Suite Authentication Bypass	Threat - widespread (0 day)	0	Remote code execution	Improper Access Control
CVE-2022-22963 Spring Cloud Function Unauthenticated Remote Code Execution (SpEL injection)	Threat - widespread (0day)	0	Cloud infrastructure compromise	Injection
CVE-2022-27593 QNAP QTS Photo Station Externally Controlled Reference	Threat - widespread (0day)	0	Network pivot	Improper Access Control
CVE-2022-41040 "ProxyNotShell" Microsoft Exchange Server Server-Side Request Forgery	Threat - widespread (0day)	0	Remote code execution	Injection
CVE-2022-41082 "ProxyNotShell" Microsoft Exchange Server Remote Code Execution	Threat - widespread (0day)	0	Remote code execution	Improper Access Control
CVE-2022-33891 Apache Spark Command Injection	Threat - widespread	4	Remote code execution	Injection
CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege "OWASSRF"	Threat - widespread	42	Remote code execution	Injection
CVE-2021-20038 SonicWall SMA 100 Series Unauthenticated Stack-Based Buffer Overflow	Threat - widespread	9*	Network pivot	Memory Corruption
CVE-2021-44228 Log4Shell Remote Code Execution in VMware vCenter Server and VMware Horizon	Threat - widespread	26	Remote code execution	Injection
CVE-2022-22954 VMware Workspace ONE Access / Identity Manager Remote Code Execution	Threat - widespread	2	Cloud infrastructure compromise	Injection
CVE-2022-22960 VMware Workspace ONE Access/Identity Manager Local Privilege Escalation	Threat - widespread	2	Local code execution	Improper Access Control
CVE-2022-29464 WSO2 File Upload Remote Code Execution	Threat - widespread	4	IT security management compromise	Injection
CVE-2022-1388 F5 BIG-IP iControl REST Authentication Bypass (RCE)	Threat - widespread	5	Network pivot	Improper Access Control
CVE-2022-22947 Spring Cloud Gateway Code Injection Vulnerability	Threat - widespread	34	Cloud infrastructure compromise	Injection
CVE-2022-30525 Zyxel Firewall Unauthenticated Remote Command Injection	Threat - widespread	1	Network pivot	Injection

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2021-4034 "Pwnkit" Linux Local Privilege Escalation	Threat - widespread	153	Local code execution	Memory Corruption
CVE-2022-26138 Hard-coded Password in Questions for Confluence Application for Confluence Server and Data Center	Threat - widespread	1	Remote code execution	Improper Access Control
CVE-2022-30333 RARLAB unRAR Directory Traversal	Threat - widespread	95	Remote code execution	Improper Access Control
CVE-2022-27925 Zimbra Collaboration Suite Directory Traversal	Threat - widespread	120**	Remote code execution	Improper Access Control
CVE-2022-26352 dotCMS Directory Traversal Remote Code Execution	Threat - widespread	Unknown	Remote code execution	Improper Access Control
CVE-2022-36804 Atlassian Bitbucket Server and Data Center Command Injection	Threat - widespread	27	Remote code execution	Injection
CVE-2022-28810 Zoho ManageEngine ADSelfService Plus Remote Command Injection	Threat - exploited in the wild (0day)	0	IT security management compromise	Injection
CVE-2022-42475 Fortinet FortiOS Heap-Based Buffer Overflow	Threat - exploited in the wild (0day)	0	Network pivot	Memory Corruption
CVE-2022-27518 Citrix ADC Arbitrary Code Execution	Threat - exploited in the wild (0day)	0	Network pivot	Improper Access Control
CVE-2022-22965 "Spring4Shell" Spring Framework WebDataBinder Remote Code Execution	Threat - exploited in the wild (0day)	0	Remote code execution	Injection
CVE-2022-26925 Microsoft Windows LSA Spoofing Vulnerability	Threat - exploited in the wild (0day)	0	IT security management compromise	Improper Access Control
CVE-2022-40139 Trend Micro Apex One Improper Validation Vulnerability	Threat - exploited in the wild (0day)	0	IT security management compromise	Improper Access Control
CVE-2022-3236 Sophos Firewall Remote Code Execution	Threat - exploited in the wild (0day)	0	Network pivot	Injection
CVE-2022-31199 Netwrix Auditor Arbitrary Code Execution	Threat - exploited in the wild	30**	IT security management compromise	Deserialization
CVE-2021-35587 Oracle Access Manager Remote Code Execution	Threat - exploited in the wild	233	IT security management compromise	Deserialization

CVE	Threat Status	Time to Known Exploitation (TTKE) in Days	Attacker Utility	Vulnerability Class
CVE-2022-26501 Veeam Backup & Replication Authentication Bypass	Threat - exploited in the wild	Unknown	IT security management compromise	Improper Access Control
CVE-2022-26318 WatchGuard Firebox and XTM Appliance Arbitrary Code Execution	Threat - exploited in the wild	4	Network pivot	Unknown
CVE-2022-0543 Redis Lua Sandbox Escape Remote Code Execution (Debian)	Threat - exploited in the wild	21	Remote code execution	Improper Access Control
CVE-2022-0847 "Dirty Pipe" Linux Local Privilege Escalation	Threat - exploited in the wild	49	Local code execution	Improper Access Control
CVE-2022-26923 Active Directory Privilege Escalation	Threat - exploited in the wild	100	IT security management compromise	Improper Access Control
CVE-2022-24112 Apache APISIX Remote Code Execution	Threat - exploited in the wild	17	Cloud infrastructure compromise	Improper Access Control
CVE-2022-35405 Zoho ManageEngine Password Manager Pro Unauthenticated Remote Code Execution	Threat - exploited in the wild	75	IT security management compromise	Deserialization
CVE-2022-1040 Sophos Firewall Authentication Bypass	Threat - exploited in the wild (0day)	0	Network pivot	Improper Access Control
CVE-2022-28219 Zoho ManageEngine ADAudit Plus Remote Code Execution	Impending threat - exploit available	N/A	IT security management compromise	Injection
CVE-2022-37393 Zimbra Collaboration Suite Root Privilege Escalation	Impending threat - exploit available	N/A	Local code execution	Improper Access Control
CVE-2022-20829 Cisco ASDM Arbitrary Code Execution via Lack of Package Signing	Impending - tooling available	N/A	IT security management compromise	Improper Access Control
CVE-2021-39144 VMware Cloud Foundation (NSX-V) XStream Remote Code Execution	Impending - exploit available	N/A	Cloud infrastructure compromise	Deserialization
CVE-2022-2992 GitLab CE/EE Remote Command Execution	Impending - exploit available	N/A	Remote code execution	Injection

** Exploitation in the wild reported privately to Rapid7*

*** Estimated*

Notes on Methodology

With very few exceptions, CVEs featured in this report were either disclosed or exploited in the wild in 2022. The CVEs we have categorized as exploited in the wild in this report are not the only vulnerabilities actively exploited during the 2022 calendar year. For example, we have excluded many browser, mobile, and host-based vulnerabilities known to be exploited in the wild (e.g., bugs in Internet Explorer, Chrome, and Firefox, or bugs in iOS and macOS). Google Project Zero has a spreadsheet of some other zero-days exploited in the wild in 2022 here, with more of a focus on browser- and host-based bugs.

CVSS scores have been removed from our dataset as of 2021. CVSS score can be a useful metric, but we believe other forms of metadata, such as threat status and attacker utility, are more important for risk assessment and prioritization than CVSS alone.

Since the trustworthiness of our data is important, we cite primary sources wherever possible for vulnerabilities we've listed as exploited in the wild—that is, we reference firsthand accounts of exploitation from the organizations or individuals who detected, verified, and reported them. Examples of primary sources referenced throughout this paper include U.S. cybersecurity and intelligence agency alerts on known exploitation; security firm analyses of threats and IOCs they've tracked during incident response or other investigations; and vendor advisories that specify exploitation in the wild (this includes CVEs that are disclosed as zero-days).

In the interest of readability, in some cases we also cite articles in security news publications that aggregate disparate reports of exploitation. This is especially useful when certain vulnerabilities, like Atlassian Confluence CVE-2022-26134 or Log4Shell CVE-2021-44228, are so widely exploited that it is helpful to see them contextualized in a single article. Our goal in citing news sources is to allow readers to understand the volume and impact of exploitation as quickly as possible.

Threat Categorization

Widespread threats are vulnerabilities under attack by many bad actors. Previously, we categorized any CVE that was leveraged by ransomware operators as a widespread threat, since ransomware is by nature an at-scale operation and relies on volume to succeed. However, we have changed this policy in 2022 to accommodate evolving statistics on targeted ransomware.

Threats categorized as "exploited in the wild" are, quite simply, not known to be broadly exploited at time of writing. It is possible that evidence of broader exploitation exists but has not been shared publicly.

Likewise, while we do not have evidence at time of writing that CVEs in **our impending threat** category are exploited in the wild, lack of evidence does not mean absence of exploitation (e.g., CVE-2022-20829, CVE-2022-28219).

Ransomware Citations

We use security news articles frequently to document ransomware operators' use of specific CVEs. Ransomware citations in this report are a binary — either there is credible technical evidence of ransomware groups' usage of a vulnerability or there is not. Lack of confirmation does not mean a CVE has not been used in ransomware operations, only that we have not seen independently verifiable details supporting that conclusion. Credible sources typically include some combination of original analysis (e.g., CVE-2021-44228, CVE-2022-31199), news articles that aggregate primary sources (CVE-2022-26134, CVE-2022-22954), and expert commentary on open platforms (CVE-2022-30190). In general, when a report comes from an individual or a little-known entity rather than a recognized expert, we look for technical information like payloads, source IPs, threat actor attribution, IOCs, and/or attack chain analysis to support the claim.

Calculating Time to Known Exploitation (TTKE)

Compiling and communicating timelines is one of the most difficult parts of risk assessment. When calculating Time to Known Exploitation (TTKE), wherever possible we will attempt to use the first credible public reference to a vulnerability's existence and the first credible public reference to exploitation in the wild. Often the first and most authoritative source on the existence of a new CVE is a vendor advisory, but in this age of widespread zero-day exploitation and public discourse, community references can pre-date vendor bulletins. The initial two ProxyNotShell vulnerabilities (CVE-2022-41040 and CVE-2022-41082) are an example of this, as is CVE-2022-37393. Rarely if ever do we use sources like the National Vulnerability Database (NVD) for disclosure baseline dates, since those dates tend to be several days or weeks behind public (and therefore attacker) knowledge.

Important note: The first known report of exploitation is just that—the first known report. It's possible, and in some cases likely, that exploitation began before a public analysis was released. TTKE data should not be taken as evidence that a vulnerability was NOT exploited before the observed date.

Glossary of Terms

Attacker Utilities

Remote code execution (RCE):
Code execution on a remote target. Typically refers to the ability to execute a payload on a target system (e.g., obtain a shell session). Aids in credential stealing, data exfiltration, and so on.

Local code execution:
The ability to run code locally on a system to which the attacker already has some access. Most commonly used to escalate privileges (e.g., by executing code as the user running the vulnerable application).

Cloud infrastructure compromise:
Remote code execution or takeover of cloud gateways or API management products (e.g., Apache APISIX, VMware Cloud Foundation, VMware vRealize Automation, Spring Cloud Gateway)

IT security management compromise:
Remote code execution or takeover of identity or access management products, including single sign-on (SSO) and AD management solutions, or other security products (e.g., Oracle Access Manager, ManageEngine Password Manager, WSO2 Identity Server, ManageEngine ADSelfService Plus, Trend Micro Apex One)

Network pivot:
The ability to pivot from an external network to an internal network, most often by exploiting internet-facing systems such as VPNs, firewalls, routers, and other gateway devices. A network pivot gives an attacker visibility into both internal and external traffic and aids in data exfiltration, traffic sniffing, and further attacks within the target network.

Social engineering:
Encompasses vulnerabilities that typically require a user to click on or preview a malicious attachment for successful exploitation to occur

Previous vulnerability intelligence reports have included lateral movement, file enumeration, and network infrastructure compromise as attacker utilities. The 2022 dataset does not include any file enumeration or lateral movement vulns, and network infrastructure compromise has been deprecated in favor of cloud infrastructure compromise and IT security management compromise.

Vulnerability Classes

Deserialization is the process through which an application is able to convert data from a portable format to data types native to its own language. Many modern languages support deserialization, including Java, .NET, Python, and Ruby. The deserialization process can pose a threat to security when the data that is loaded into the native language can be tampered with by a malicious party. Typical attacks involve configuring the data to invoke a method with the arguments necessary to execute an operating system command. This results in command execution in the context of the loading application. Common solutions to this security problem include cryptographically signing the data to ensure its authenticity and utilizing an allowlist of data types that are permitted to be loaded. Associated CWEs: CWE-502.

Improper Access Control refers to a missing or insufficient access control to a particular interface into a system (most often a remotely accessible API). Improper uses of cryptography for the purpose of authentication also fall under this vulnerability class. Common solutions to this problem include proper authentication, authorization, and accounting implementations for all sensitive interfaces, as well as secure management of all related secrets. A non-exhaustive list of associated CWEs: CWE-285, CWE-200, CWE-287, CWE-732.

Memory Corruption is a large category of vulnerabilities that involve the misuse of data through a variety of means to alter memory and produce unexpected behavior. This vulnerability class includes improper boundary enforcement, type confusion, uninitialized data use, and the use of data after it has been freed, to name a few. These vulnerabilities often manifest themselves in languages that are not considered memory-safe. Successful exploitation of memory corruption vulnerabilities can result in arbitrary code execution within the context of the running application, or in an unhandled exception that causes the application to crash and triggers a denial of service (DoS) condition. Common solutions to this problem typically involve additional validation on parameters to key operations, such as those used to load and store data. Successful exploitation of these classes of vulnerabilities has become more complex in recent years due to the variety of mitigation technologies that have been developed for operating systems, compilers, and applications (e.g., kASLR, Control Flow Guard, win32k Type Isolation). A non-exhaustive list of associated CWEs: CWE-787, CWE-125, CWE-416, CWE-190, CWE-476.

Injection is a large category of vulnerabilities involving specially crafted input that is interpreted in a particular way by an associated system. Most commonly seen in web applications, injection attacks are often more specifically labeled by the type of data being interpreted (e.g., SQL, LDAP, OS commands). The root cause of these vulnerabilities is almost always insufficient sanitization on data received from a malicious party. Exploitation of these vulnerabilities tends to be reliable, rarely resulting in service degradation unless intended (such as through SQL or OS commands). Our 2021 report includes JNDI, OGNL, SSRF, and other techniques we have classified as injection flaws in addition to traditional OS and SQL command injection vulnerabilities.

The context under which the logic is executed typically depends on how it is interpreted. In the case of a web application, for example, SQL injection may be executed on a back-end database server, while OS commands are injected on the front-end web server, and JavaScript is executed by the end user's browser. This class of vulnerabilities is therefore unique in that it commonly involves a vulnerability in one system compromising the integrity of others. Common solutions to this problem typically involve implementing strict sanitization on parameters though the use of allowlists. A non-exhaustive list of associated CWEs: CWE-79, CWE-20, CWE-89, CWE-94.

References

Security research is a community pursuit. This report benefited from the work of many individual researchers and research teams, including but not limited to the work of the folks listed below:

Aaron Soto and Jon Hart, Rapid7 (2019)

Adam Janofsky, The Record, Recorded Future News (2022)

Andreas Klopsch, Sophos X-Ops (2022)

Andrew Case, Sean Koessel, Steven Adair, Thomas Lancaster, Volexity Threat Research (2022)

Anuj Soni and Ryan Chapman, BlackBerry (2022)

Akamai Threat Research Team (2022)

Asheer Malhotra, Cisco Talos (2022)

Avertium (2022)

Bishop Fox (2022)

Brian Pitchford, Erik Iker, Nicolas Zilio, CrowdStrike (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Condon, Rapid7 (2022)

Caitlin Huey, Cisco Talos (2022)

Cara Lin, Fortinet (2022)

Carl Windsor, Fortinet PSIRT Blogs (2022)

Carly Page, TechCrunch (2022)

Christoper Ordonez and Alvin Nieto, Trend Micro (2022)

Christophe de la Fuente, Rapid7 (2023)

Cisco (2022)

Cisco Talos (2022)

CISA Cyber Safety Review Board (2022)

CISA Known Exploited Vulnerabilities Catalog (2022)

Citrix Support Knowledge Center (2022)

Clayton Zechman, Rapid7 (2022)

CloudSEK Threat Intelligence (2022)

Confluence Security Advisory (2022)

Connor Jones, ITPro (2022)

Dan Goodin, Ars Technica (2022)

Dan Goodin, Ars Technica (2022)

Dan Goodin, Ars Technica (2022)

Danny Palmer, ZDNet (2022)

Danny Palmer, ZDNet (2022)

Danny Palmer, ZDNet (2022)

Darren Martyn (2021)

Darren Martyn (2021)

Don Ovid Ladores, Lucas Silva, Scott Burden, Janus Agcaoili, Ivan Nicole Chavez, Ian Kenefick, Ieriz Nicolle Gonzalez, and Paul Pajares, Trend Micro (2022)

The Economist (2022)

Eduard Kovacs, Security Week (2022)

Emsisoft Malware Lab (2023)

Eoin Miller, Rapid7 (2022)

Erick Galinkin, Rapid7 (2022)

Erick Galinkin, Rapid7 (2022)

ESET (2022)

F5 (2022)

FortiGuard Labs PSIRT Advisories (2022)

Fortinet PSIRT (2022)

Glenn Thorpe, Rapid7 (2022)

Glenn Thorpe, Rapid7 (2022)

Glenn Thorpe, Rapid7 (2022)

Glenn Thorpe, Rapid7 (2022)

Global Research and Analysis Team, Kaspersky Securelist (2022)

Google Project Zero (2022)

Grant Willcox, Rapid7 (2022)

Grant Willcox, Rapid7 (2022)

Grant Willcox, Rapid7 (2021)

GreyNoise Intelligence (2022)

GreyNoise Intelligence (2022)

The GreyNoise Team, GreyNoise Intelligence (2022)

GTSC (2022)

Hanko van Giessen (h00die-gr3y) (2022)

Hanko van Giessen (h00die-gr3y) (2022)

Hanko van Giessen (h00die-gr3y) (2022)

Heyder Andrade (2022)

Hilary Whiteman, CNN (2022)

Insikt Group, The Record, Recorded Future News (2022)

Ionut Ilascu, Bleeping Computer (2022)

Ivanti Ransomware Index Update Q2-Q3 2022 (2022)

Jaeson Schultz, Cisco Talos (2022)

Jack Heysel, Rapid7 (2022)

Jake Baines (2023)

Jake Baines (2021)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2022)

Jake Baines, Rapid7 (2021)

Jake Baines, Rapid7 (2022)

James Pearson and Raphael Satter, Reuters (2022)

Jeff Stone, Bloomberg (2022)

Jie Ji, NSFOCUS (2022)

Jim Walter, SentinelOne Blog (2022)

Joe Uchill, SC Magazine (2022)

John Dunn, ransomware.org (2022)

Jon Gold, CSO (2022)

Jonathan Greig, The Record, Recorded Future News (2022)

Jonathan Greig, The Record, Recorded Future News (2022)

Jonathan Greig, The Record, Recorded Future News (2022)

Jonathan Lloyd, NBC Los Angeles (2022)

Jonathan Munshaw, Cisco Talos (2022)

Jonathan Reid, Security Intelligence (2022)

Kaspersky (2022)

Keith Wojcieszek, Stephen Green, Elio Biasiotto, Kroll (2022)

Kevin Beaumont, DoublePulsar (2022)

Kevin Beaumont, DoublePulsar (2022)

Larry Cashdollar, Akamai (2022)

Lawrence Abrams, Bleeping Computer (2022)

Lawrence Abrams, Bleeping Computer (2022)

Lawrence Abrams, Bleeping Computer (2022)

Lindsey O'Donnell-Welch, Decipher (2022)

Lucian Constantin, CSO (2022)

Lucian Constantin, CSO (2022)

Malwarebytes Labs (2022)

Malwarebytes Threat Intelligence (2022)

ManageEngine ADAudit Plus (2022)

ManageEngine ADSelfService Plus (2022)

Matthew Remacle, GreyNoise Intelligence (2023)

Michal Poslušný, ESET (2022)

Microsoft (2022)

Microsoft Defender Threat Intelligence (2022)

Microsoft Defender Threat Intelligence and Microsoft Threat Intelligence Center (2022)

Microsoft Security Intelligence (2022)

Microsoft Security Intelligence (2022)

Microsoft Security Response Center (2022)

Microsoft Security Response Center (2022)

Microsoft Security Response Center (2022)

Microsoft Security Response Center (2022)

Microsoft Security Response Center (2022)

Microsoft Security Response Center (2022)

Microsoft Security Threat Intelligence (2022)

Microsoft Update Catalog (2022)

Microsoft Windows Driver Store (2021)

MITRE (2022)

Morphisec Labs (2022)

Morphisec Labs (2022)

NHS Digital (2022)

Nikolay Pankov, Kaspersky (2018)

Nitesh Surana and Ashish Verma, Trend Micro (2022)

noraj (2022)

Ofer Caspie, AT&T Cybersecurity Blog (2022)

Oliver Lyak, Danish Institute for Cyber Risk (2022)

Olympe Cyberdefense (2022)

Patrick Bennett, CrowdStrike (2022)

Paul Kimayong, Juniper Networks (2022)

Phil Muncaster, Infosecurity Magazine (2022)

Pierluigi Paganini, Security Affairs (2022)

Pieter Arntz, Malwarebytes Labs (2022)

ProjectDiscovery (2022)

QNAP (2022)

Ram Gall, Wordfence (2022)

Rapid7 (2022)

Rapid7 (2022)

Rapid7 (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2021)

Rapid7 AttackerKB (2021)

Rapid7 AttackerKB (2021)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2020)

Rapid7 AttackerKB (2020)

Rapid7 AttackerKB (2020)

Rapid7 AttackerKB (2020)

Rapid7 AttackerKB (2021)

Rapid7 AttackerKB (2022)

Rapid7 AttackerKB (2022)

Ravie Lakshmanan, The Hacker News (2022)

Ravie Lakshmanan, The Hacker News (2022)

Ravie Lakshmanan, The Hacker News (2022)

Ravie Lakshmanan, The Hacker News (2022)

remy (2022)

remy (2022)

Riam Kim-McLeod, Digital Shadows (2022)

RiskIQ Threat Intel Portal (2022)

Rob Joyce, U.S. National Security Agency (2022)

Robert Knapp, Rapid7 (2022)

Ron Bowes, Rapid7 (2022)

Ron Bowes, Rapid7 (2022)

Ron Bowes, Rapid7 (2022)

Ron Bowes, Rapid7 (2022)

Ruchna Nigam, Palo Alto Networks Unit 42 (2022)

SANS.edu Internet Storm Center (2022)

Sergiu Gatlan, Bleeping Computer (2022)

Sergiu Gatlan, Bleeping Computer (2022)

Sergiu Gatlan, Bleeping Computer (2022)

Sergiu Gatlan, Bleeping Computer (2022)

Sergiu Gatlan, Bleeping Computer (2022)

Shadowserver (2022)

Shadowserver (2022)

Shelby Pace, Rapid7 (2022)

Slashdot (2023)

Sophos (2022)

Spencer McIntyre, Rapid7 (2022)

Spencer McIntyre, Rapid7 (2022)

Spencer McIntyre, Rapid7 (2022)

Spencer McIntyre, Rapid7 (2022)

Spencer McIntyre, Rapid7 (2023)

Spencer McIntyre, Rapid7 (2023)

Spring by VMware Tanzu (2022)

Spring Cloud (2022)

The Stack (2022)

Stephen Weigand, SC Magazine (2022)

Steven Adair, Thomas Lancaster, Volexity Threat Research (2022)

Sunil Bharti, Trend Micro (2022)

Susan Bradley, CSO (2022)

Tiago Henriques (2022)

Tiago Pereira, Cisco Talos (2022)

Tod Beardsley, Rapid7 (2022)

Tod Beardsley, Rapid7 (2022)

Trend Micro Security Bulletin (2022)

Trend Micro Research (2022)

Tushar Richabadas, Barracuda (2022)

UMass Boston (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Cybersecurity and Infrastructure Security Agency (2022)

U.S. Department of State (2022)

U.S. National Security Agency (2022)

VMware (2022)

VMware (2022)

Volexity Threat Research (2022)

WatchGuard Internet Security Report Q2 2022 (2022)

Will Schroeder, SpecterOps (2021)

William Bowling (2022)

XStream (2022)

yeak (2022)

Zack Allen, Frederic Baguelin, Emile Spir, Eslam Salem, Datadog Security Labs (2022)

Zeljka Zorz, Help Net Security (2022)

Zscaler Threatlabz (2022)

POWER TO THE PROTECTORS

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/