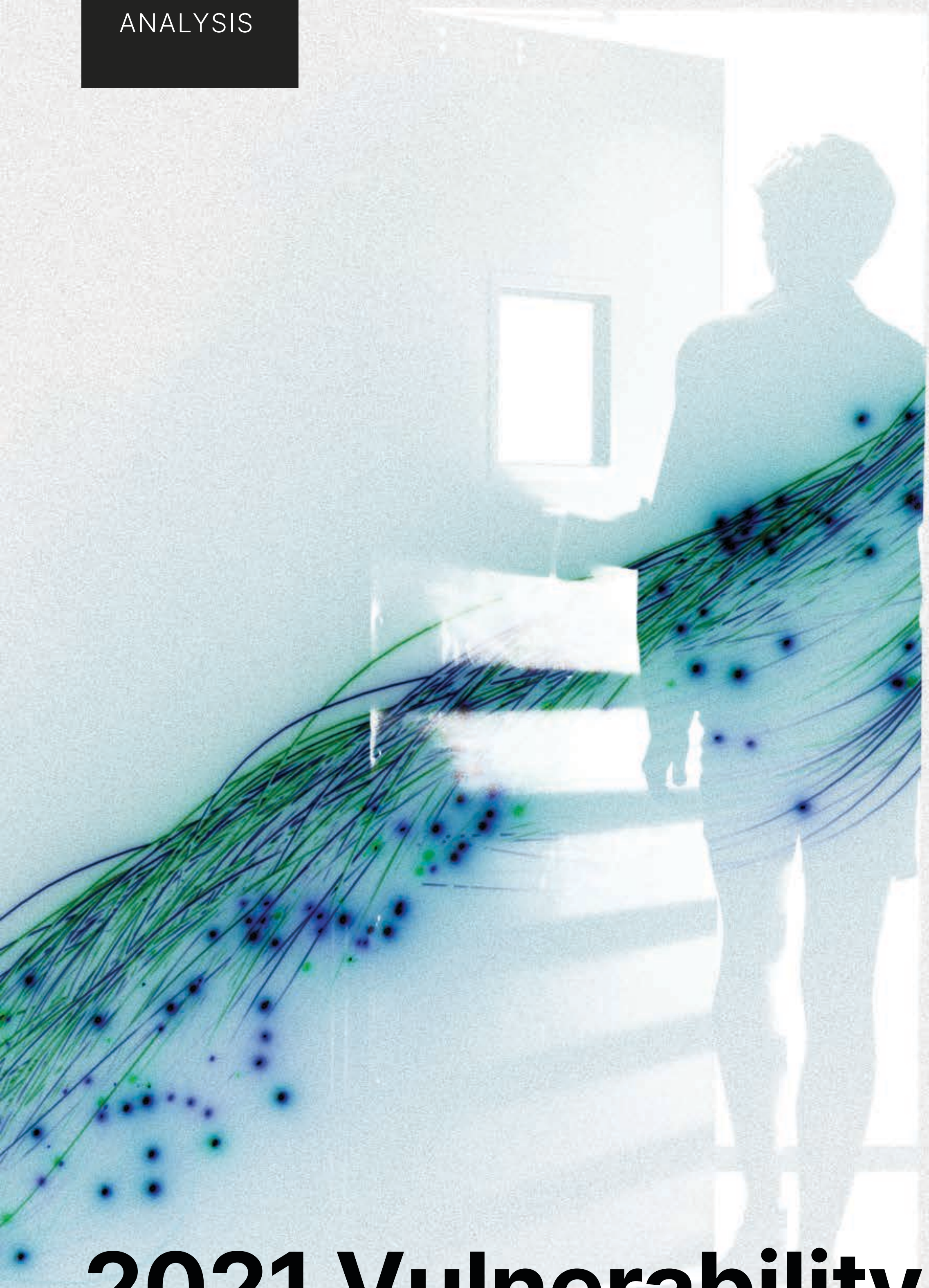
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

February 10, 2022



2021 Vulnerability Landscape

The annual vulnerability report surveys the threat landscape of 2021, summarizing a year of intelligence produced by Recorded Future's threat research team, Insikt Group. It draws from data on the Recorded Future® Platform, including open sources like media outlets and publicly available research from other security groups, as well as closed sources on the criminal underground, to analyze global trends and evaluate the top 10 most significant vulnerability disclosures from 2021. The report will be of interest to anyone seeking a broad, holistic view of the cyber vulnerability threat landscape in 2021.

Executive Summary

The 2021 vulnerability threat landscape was defined by high-profile incidents involving integral vendor software that led to widespread data breaches and malware attacks. With timing reminiscent of the SolarWinds Orion SUNBURST backdoor disclosure in December 2020, the most serious vulnerability of 2021, commonly known as "Log4Shell" and tracked as CVE-2021-44228, was first publicly disclosed on December 9, 2021. Other major vulnerabilities throughout the year were identified affecting Microsoft Exchange and Windows Print Spoolers, VMware vCenter, legacy Accellion FTA, and the IT management company Kaseya's Virtual System Administrator. Each of these critical vulnerabilities were exploited by criminal and state-sponsored threat actors in compromises including data breaches and ransomware attacks that had far-reaching consequences for vendors in all industry tiers.

The severity of many of the disclosed and exploited vulnerabilities in 2021, particularly the Log4Shell vulnerabilities and the numerous vulnerabilities associated with Microsoft technologies, should not distract from the number and diversity of affected products throughout 2021. High-risk vulnerabilities and actively exploited vulnerabilities disclosed in 2021 affected products belonging to a more diverse array of parent companies than prior years. Outside of the top 10, which mainly affected Microsoft products, serious actively exploited vulnerabilities were also identified affecting products from Linux, Google, Pulse Connect Secure, and Apple, among others.

Several of these vulnerabilities were initially exploited in zero-day attacks, as they had already been targeted prior to discovery and disclosure, or in N-day attacks, in which the vulnerability is known but a patch is unavailable. In addition, shortly after vulnerability disclosures, threat groups hastily targeted vulnerable systems to deploy post-exploitation malware and malicious tools.

Contrary to our findings in previous years (2020, 2019, 2018), none of the top exploited vulnerabilities of 2021 were recycled vulnerabilities disclosed in prior years. Rather, the notable trend in 2021 vulnerability exploitation on the criminal underground was how quickly threat actors have begun exploiting newly discovered vulnerabilities in the wild and deploying post-exploitation tools.

2021	2020	2019
1. CVE-2021-44228	1. CVE-2019-19781	1. CVE-2018-15982
2. CVE-2021-22005	2. CVE-2020-1472	2. CVE-2018-8174
3. CVE-2021-34527	3. CVE-2019-11510	3. CVE-2017-11882
4. CVE-2021-1675	4. CVE-2020-0796	4. CVE-2018-4878
5. CVE-2021-27065	5. CVE-2017-11882	5. CVE-2019-0752
6. CVE-2021-36934	6. CVE-2020-0674	6. CVE-2017-0199
7. CVE-2021-40444	7. CVE-2019-1367	7. CVE-2015-2419
8. CVE-2021-26855	8. CVE-2012-0158	8. CVE-2018-20250
9. CVE-2021-22205	9. CVE-2020-14882	9. CVE-2017-8750
10. CVE-2021-21551	10. CVE-2019-1458	10. CVE-2012-0158
2018	**2017**	**2016**
1. CVE-2018-8174	1. CVE-2017-0199	1. CVE-2016-0189
2. CVE-2018-4878	2. CVE-2016-0189	2. CVE-2016-1019
3. CVE-2017-11882	3. CVE-2017-0022	3. CVE-2016-4117
4. CVE-2017-8750	4. CVE-2016-7200	4. CVE-2015-8651
5. CVE-2017-0199	5. CVE-2016-7201	5. CVE-2016-0034
6. CVE-2016-0189	6. CVE-2015-8651	6. CVE-2016-1010
7. CVE-2017-8570	7. CVE-2014-6332	7. CVE-2014-4113
8. CVE-2018-8373	8. CVE-2016-4117	8. CVE-2015-8446
9. CVE-2012-0158	9. CVE-2016-1019	9. CVE-2016-3298
10. CVE-2015-1805	10. CVE-2017-0037	10. CVE-2015-7645

Table 1: Top exploited vulnerabilities between 2016 and 2021, with repeats designated by color. (Source: Recorded Future)

2021 Vulnerability Landscape Overview

According to data from the US National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), 21,957 vulnerabilities were published to the NVD in 2021. Comparing the increase in new disclosures since 2017, 2021 showed a threefold increase in the margin of difference from 2019 to 2020. The ever-growing number of disclosed vulnerabilities has rendered vulnerability tracking and prioritization efforts increasingly difficult, placing security teams at a disadvantage relative to their attackers. However, of the 16,473 newly disclosed vulnerabilities with a CVE designator of 2021 listed in the NVD database, only 119 (0.7%) of these vulnerabilities are known to have been actively exploited (per the CISA Known Exploited Vulnerabilities Catalog). This major discrepancy between overall disclosures and actual exploitation shows how security teams can use Recorded Future's Platform data to quickly identify vulnerabilities with high risk scores and triggered risk rules indicating active exploitation to facilitate patch prioritization and remediation efforts.

In the first half of 2021, attackers ignored consumer-grade software in favor of technology normally used by business clients. In our report for the top 10 vulnerabilities of 2020 based on criminal interest, we found that many of the vulnerabilities exploited in the last several years are associated with software used by the average IT consumer, such as CVE-2017-11882 in Microsoft Office. However, throughout the first half of 2021, the main trend in exploitation was that of either business- or enterprise-class technology, such as Microsoft Exchange and VMware vCenter. Enterprise-grade, high-value software was increasingly targeted by threat actors, introducing the threat of exponentially higher costs associated with cyberattacks. Likewise, many of these major vulnerabilities centered on a relatively new but rapidly expanding field: cloud-based technologies.

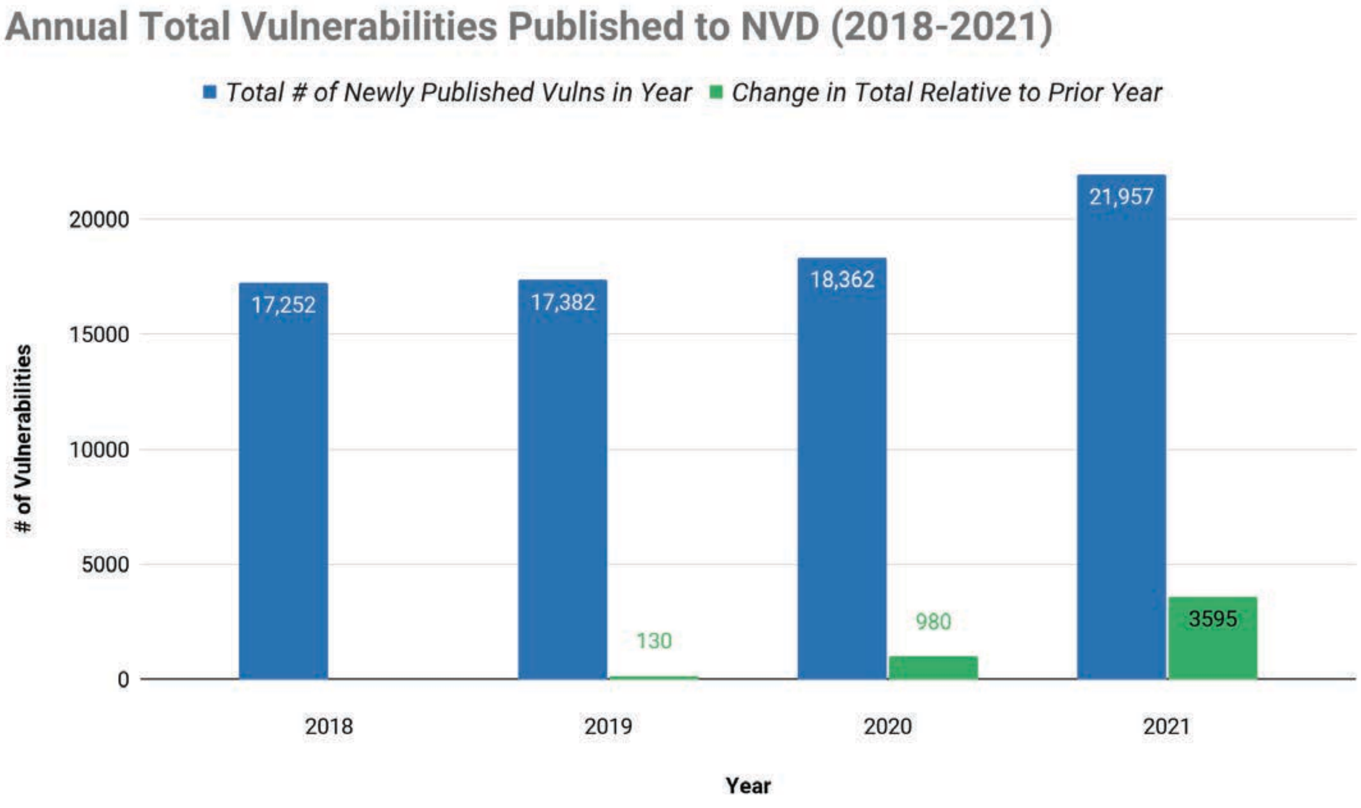


Figure 1: Annual total number of vulnerabilities published to the NVD, 2018 to 2021. Note: Annual totals include any vulnerability with a release date that fell within a specified year, which may differ from the year listed within a CVE ID. (Source: NIST NVD)

In the second half of 2021, the increase in vulnerabilities affecting enterprise-class products appeared to subside as several high-profile vulnerabilities targeting consumer-grade technology were disclosed. These included the Apple iOS vulnerability CVE-2021-30860. Citizen Lab researchers linked CVE-2021-30860 to the "ForcedEntry" exploit used to deliver the Pegasus spyware developed by Israel-based cybersecurity company NSO Group to the iPhones of activists in Bahrain and Saudi Arabia. In December 2021, Reuters disclosed that CVE-2021-30860 was also exploited in attacks against 9 employees of the US State Department.

Late in 2021, Log4Shell shook the security landscape for individual consumers and major enterprises, affecting a huge range of systems. Log4Shell underscores the most alarming trends in the 2021 vulnerability landscape: the ever-shrinking window for remediation between initial vulnerability disclosures and attacker exploitation and ongoing zero-day vulnerability exploitation by both cybercriminals and nation-state threat actors.

Top 10 Vulnerabilities Disclosed in 2021

The top 10 vulnerabilities are determined based on multiple factors, including CVSS v3.1 and Recorded Future risk score ratings, proof-of-concept (PoC) weaponization and exploitation, and the number of references to distinct cyberattacks. The top 10 are listed below from highest to lowest threat as assessed via the methodology outlined above, followed by the affected product and vulnerability type.

1. CVE-2021-44228 (Log4Shell): Apache Log4j2 - Remote Code Execution (RCE)
2. CVE-2021-22005: VMware vCenter Server - Arbitrary File Upload
3. CVE-2021-34527 (PrintNightmare): Windows Print Spooler - RCE
4. CVE-2021-1675 (PrintNightmare): Windows Print Spooler - Elevation of Privilege
5. CVE-2021-27065 (ProxyLogon): Microsoft Exchange Server - RCE
6. CVE-2021-36934: Windows - Elevation of Privilege
7. CVE-2021-40444: Microsoft MSHTML - RCE
8. CVE-2021-26855 (ProxyLogon): Microsoft Exchange Server - RCE
9. CVE-2021-22205: GitLab CE/EE - Remote Code Execution
10. CVE-2021-21551: Dell - Insufficient Access Control

Apache Log4j

Widely considered one of the worst security flaws in recent memory, CVE-2021-44228 (commonly known as Log4Shell) has upended the cybersecurity world in a matter of weeks and is the top vulnerability disclosure of 2021. The vulnerability resides in Apache's Log4j, a software logging library written in Java. Log4Shell is so damaging because it combines ease of exploitation, allowing attackers remote access, with the almost ubiquitous use of Log4j across networks and applications.

Background

Much in the same way that asbestos use was commonplace in mid-20th century building construction, Log4j is incorporated into many software and networking applications today. And like asbestos in a wall, when left undisturbed, the vulnerability is not actively damaging; once exploited, however, Log4Shell poses a critical threat to affected systems. Its general use means this threat is spread across a huge potential attack surface, comprising each individual unpatched system, any of which are at significant risk of exploitation that could present a threat to both the target and associated third parties.

Compounding the general threat posed by Log4Shell, remediation efforts for the vulnerability were complicated by a series of insufficient patches (2.15.0 for the initial vulnerability CVE-2021-44228, 2.16.0 for CVE-2021-45046, 2.17.0 for CVE-2021-45105, and 2.17.1 for CVE-2021-44832), which introduced new vulnerabilities that allow for denial of service and even introduced an arbitrary code execution vulnerability. Organizations that have not yet patched the vulnerability should be updating Log4j to version 2.17.1.

Active Exploitation of Log4Shell Vulnerabilities

Several threat groups have begun rapidly exploiting the Log4Shell vulnerabilities since their disclosure. These include ransomware operators, such as Conti, Khonsari, and TellYouThePass [1, 2], as well as nation-state actors. According to Cisco Talos, Log4Shell exploitation likely began as early as December 1 and December 2, 2021, suggesting the vulnerability was being exploited in the wild for at least a week before its public disclosure. Recorded Future observed scanning and exploitation behavior beginning within hours of the vulnerability disclosure, nearly all from the Tor network, and by December 10, the day after its initial disclosure, Imperva reported 1.4 million attempts to scan for the vulnerability.

Most of these early attacks originated from threat actors deploying cryptomining malware and botnets, including Mirai, Muhstik, and Kinsing. On December 14, 2021, Microsoft researchers confirmed that CVE-2021-44228 was being used by multiple state-sponsored threat activity groups originating from China (HAFNIUM), Iran (PHOSPHORUS), North Korea, and Turkey to deploy web shells and the often-weaponized penetration-testing tool Cobalt Strike. By January 4, 2022, attackers were observed exploiting the vulnerability in internet-facing systems running VMware Horizon (a proof of concept was later shared via GitHub) to deploy the NightSky ransomware.

Remediation and the Future of Log4Shell

Since Apache first disclosed the Log4Shell vulnerability on December 9, 2021, security teams worldwide have been rapidly working to identify and patch vulnerable systems and remediate potential intrusions. In nearly unprecedented cooperative remediation efforts, security organizations, such as GreyNoise, BadPackets, Huntress Labs, and Curated Intel, have offered their services to identify and monitor for Log4Shell indicators of compromise. Cloudflare stated that the damage potential is so great that it is introducing proactive mitigation measures, even for non-paying organizations.

Security teams should prioritize identifying vulnerable systems and suspicious traffic and updating vulnerable systems using Java 8 and Log4j to version 2.17.1. Additional background on the Log4Shell vulnerabilities and guidance on hunting for traffic attempting to exploit Log4j is available in this blog post. Organizations can also track updates to the Log4Shell vulnerability by following updates published by CISA [1, 2] as this situation continues to evolve rapidly.

Cloud Vulnerabilities

The increased targeting and exploitation of vulnerabilities affecting cloud technologies, a trend that began in earnest in 2020, continued and grew in 2021. In response to the pandemic in 2020, remote work grew rapidly, which caused a sharp uptick in enterprise and individual consumer reliance on cloud-based IT services in 2020 and 2021. According to statistics tracked by IDC, the worldwide market for all cloud infrastructure (shared and dedicated) surpassed that of non-cloud infrastructure in 2020. By 2022, the market for shared cloud infrastructure alone is expected to surpass that of non-cloud infrastructure. By 2025, cloud infrastructure is forecast to account for nearly two-thirds of the entire enterprise infrastructure market.

The increasing adoption of cloud-based technologies has been accompanied by a rise in serious vulnerabilities affecting these systems, such as the second vulnerability on 2021's top 10 list, CVE-2021-22005, which affected VMware's vCenter servers. Furthermore, as the number of internet-of-things (IoT) enabled devices continues to expand, defenders face increasingly difficult tensions involving vulnerability remediation between cloud-based and on-premises technologies.

Case Study: VMware

The VMware vCenter vulnerability CVE-2021-22005 exemplifies the rapid exploitation of newly disclosed vulnerabilities. VMware published an advisory on September 21, 2021, that included a patch and workaround for CVE-2021-22005, an arbitrary file upload vulnerability that can enable RCE. A day after CVE-2021-22005 was disclosed, the threat intelligence company Bad Packets posted on social media that threat actors were already exploiting the vulnerability via VMware honeypots, as attacks originated from the US, Canada, Romania, China, the Netherlands, and Singapore.

The Vietnamese security researcher Nguyen Jang shared his PoC script targeting CVE-2021-22005, based on the workaround and patch released by VMware 3 days after disclosure. The same day the PoC was published, CISA issued an advisory urging organizations and users to apply the patch or implement the available workaround provided by VMware. Although Jang's PoC script was an "incomplete" exploit, intentionally missing the code leading to RCE to prevent less skilled threat actors from using the PoC in attacks, an increase in exploit activity for CVE-2021-22005 was observed the day after the PoC was published and several threat actors were detected using the code Jang had released in the following weeks.

Microsoft

Microsoft technologies have a reputation [1, 2] for being riddled with vulnerabilities and have been frequent targets for threat actor exploitation; 6 of the top 10 vulnerabilities in 2021 affected Microsoft products. Several Microsoft vulnerabilities disclosed in 2021 — particularly the ProxyLogon and ProxyShell vulnerabilities, which affect Exchange Servers, and the PrintNightmare vulnerabilities, which affect the Windows Print Spooler — were weaponized by both cybercriminals and nation state-sponsored threat groups. Although 2021 saw a rise in exploitation of vulnerabilities affecting all major operating systems (serious actively exploited vulnerabilities in 2021 were also found affecting Apple iOS and Debian Linux), Microsoft Windows continues to be the most heavily targeted OS.

Case Study: Microsoft Exchange

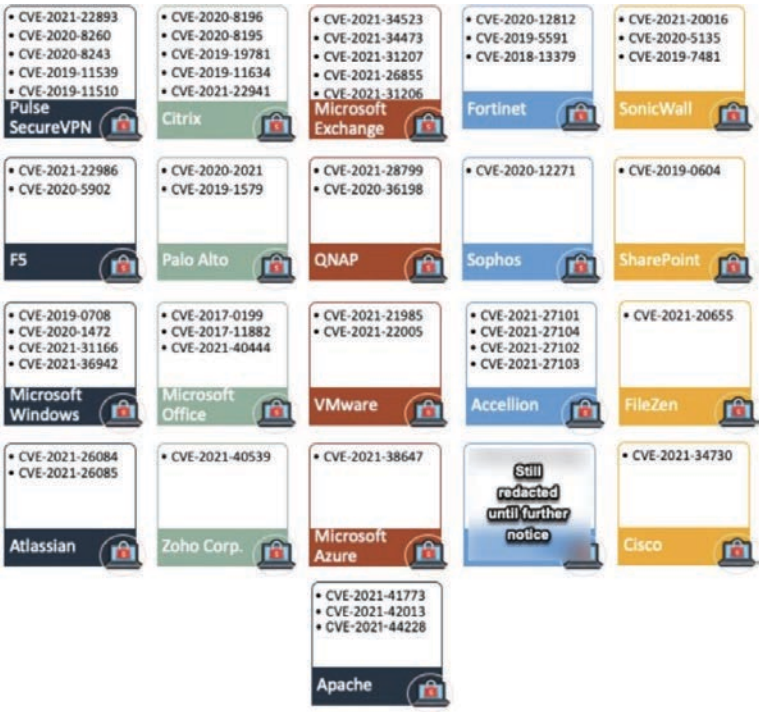
On March 2, 2021, Microsoft disclosed that the APT group HAFNIUM had exploited 4 Microsoft Exchange Server vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) to install web shells. Throughout March 2021, the number of victims, attackers, and malware associated with the exploitation of these Microsoft Exchange Server vulnerabilities grew widely, and affected organizations included local government bodies, a university, an engineering company, and retailers. A PoC exploit for ProxyLogon, the name given to CVE-2021-26855 (the top 8 vulnerability in 2021) when chained with CVE-2021-27065 (the top 5 vulnerability), was publicly released on GitHub on March 10, 2021, and was quickly shared on other sources.

Since their disclosure, these vulnerabilities have been exploited by at least 10 other APT groups or activity clusters, including Tick, LuckyMouse, Calypso, Websiic, Winnti Group, and Tonto Team. In addition to these APT groups, other attackers that were later seen [1, 2] exploiting these vulnerabilities included the operators of the DearCry ransomware and Black Kingdom ransomware, among others.

On August 19, 2021, Huntress Labs discovered that threat actors were actively exploiting [1, 2] Microsoft Exchange servers via the ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207), which allow for remote code and arbitrary code execution. Huntress Labs observed threat actors were deploying 5 distinct styles of web shells to vulnerable Exchange servers in August 2021, with more than 100 incidents reported related to these exploits between August 17 and 18, 2021, alone. Operators of LockFile ransomware, which first surfaced in July 2021, were also observed exploiting the 3 ProxyShell vulnerabilities soon after their disclosures, between May and July 2021, well within the mean time for remediation of internet-facing vulnerabilities (60 days).

Ransomware Vulnerability Exploitation

As mentioned in the case studies highlighted previously in this report, ransomware operations leaned heavily on vulnerability exploitation in 2021. Major ransomware operations showed a particular interest in vulnerabilities that could cause widespread damages to third parties or entire supply chains. Most notably, when the REvil ransomware operators exploited the zero-day Kaseya Virtual System Administrator (VSA) vulnerability CVE-2021-30116, the group also set a new precedent in ransomware resourcing, as REvil became the first ransomware operation to exploit a zero-day vulnerability as part of a major supply-chain attack. Major ransomware campaigns in 2021 also targeted vulnerabilities affecting a wide variety of other technologies, including the Log4Shell vulnerability, Microsoft's Exchange servers, and the Pulse Connect Secure VPN, among others listed in Figure 2 below.



Pulse SecureVPN
- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Citrix
- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634
- CVE-2021-22941

Microsoft Exchange
- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855
- CVE-2021-31206

Fortinet
- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

SonicWall
- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

F5
- CVE-2021-22986
- CVE-2020-5902

Palo Alto
- CVE-2020-2021
- CVE-2019-1579

QNAP
- CVE-2021-28799
- CVE-2020-36198

Sophos
- CVE-2020-12271

SharePoint
- CVE-2019-0604

Microsoft Windows
- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Office
- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444

VMware
- CVE-2021-21985
- CVE-2021-22005

Accellion
- CVE-2021-27101
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

FileZen
- CVE-2021-20655

Atlassian
- CVE-2021-26084
- CVE-2021-26085

Zoho Corp.
- CVE-2021-40539

Microsoft Azure
- CVE-2021-38647

Still redacted until further notice

Cisco
- CVE-2021-34730

Apache
- CVE-2021-41773
- CVE-2021-42013
- CVE-2021-44228

Figure 2: Vulnerabilities abused by ransomware actors (Source: Twitter)

Case Study: Kaseya VSA

On July 2, 2021, IT management company Kaseya announced a REvil (also known as Sodinokibi) ransomware attack affecting users of their VSA due to a zero-day vulnerability, CVE-2021-30116. On July 5, 2021, REvil Gang, the operators of the extortion website Happy Blog, claimed responsibility for the attack in a post titled “KASEYA ATTACK INFO”, stating that they infected “more than a million systems”. According to Recorded Future’s news media outlet, The Record, this supply-chain attack is the “largest ransomware outbreak carried out by a cybercrime gang”, affecting at least 50 managed service provider (MSP) customers of Kaseya and consequently between 800 and 1,500 businesses serviced by these MSPs.

Kaseya obtained a decrypter from a third party to help their customers recover their encrypted data, and they held a firm stance in an update on July 26, 2021, that they did not pay a ransom to obtain the decrypter. Kaseya has released a patch to address several vulnerabilities in on-premise VSA systems, and CISA published an advisory urging Kaseya VSA customers to use a Compromise Detection Tool to identify any indicators of compromise and providing guidance and best practices to harden systems against potential exploitation.

Outlook

The trend of rapid vulnerability exploitation underlines the significance of a robust and efficient vulnerability management program. CVSS scores can help defenders prioritize the likelihood that a vulnerability will be exploited, as in-the-wild exploitation is far more likely to occur with vulnerabilities that allow network exploitation and have low attack complexity or for which a PoC is readily available. However, while defenders are monitoring emerging vulnerabilities to patch, threat actors are at the same time seeking to exploit them. To this point, many of the critical vulnerability exploitations in 2021 involved zero-day vulnerabilities that even the most efficient patch-management programs would not have addressed before exploitation. Simply maintaining awareness of recent vulnerability disclosures is far less effective than implementing a combined program of tech stack auditing, defense-in-depth, and patch prioritization.

As we saw with the Microsoft Exchange server incidents in March 2021, the VMware vCenter vulnerability exploitation in September 2021, and more recently via the ongoing exploitation of the Log4Shell vulnerabilities, attackers have also been increasingly quick to target N-day security vulnerabilities as soon as they are publicly disclosed. While the LockFile operators exploited the ProxyShell vulnerabilities well within the 60-day mean time to remediate, the first mass-scanning for both the vCenter server vulnerability CVE-2021-22005 and the Log4Shell vulnerability occurred within just 24 hours of their initial public disclosures. In the case of Log4Shell, strong evidence suggests that the vulnerability was being exploited as a zero-day up to a week in advance of the first public reports.

Further highlighting the urgency surrounding prompt remediation for actively exploited vulnerabilities, on January 4, 2022, the US Federal Trade Commission issued a press release stating that the agency intends to begin taking legal actions against companies who fail to protect consumer data by not patching applications vulnerable to Log4Shell. While patching processes are complicated, prioritization based on threat intelligence can prevent a lawsuit and be the difference between a significant security breach and a detected and defended breach attempt.

Vulnerability Remediation Resources

The table below provides links to remediation sources for the top 10 exploited vulnerabilities in this report.

Rank	CVE	Remediation	CVSS	Recorded Future Risk Score
1	**CVE-2021-44228**	https://logging.apache.org/log4j/2.x/security.html	10	99
2	**CVE-2021-22005**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	9.8	99
3	**CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	8.8	99
4	**CVE-2021-1675**	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675	8.8	99
5	**CVE-2021-27065**	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065	7.8	99
6	**CVE-2021-36934**	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36934	7.8	99
7	**CVE-2021-40444**	https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40444	7.8	99
8	**CVE-2021-26855**	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855	9.8	99
9	**CVE-2021-22205**	https://gitlab.com/gitlab-org/gitlab/-/issues/327121	10	99
10	**CVE-2021-21551**	https://www.dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability	7.8	89

Table 2: Remediation resources for the top 10 vulnerabilities of 2021

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About the Author

Joanna Oxley

Associate Threat Intelligence Analyst, Insikt Group®

Joanna Oxley is an Associate Threat Intelligence Analyst on the Subscriptions and Periodicals team within Recorded Future's analyst-on-demand services and threat research division, Insikt Group. She holds a Master of Science in Cybersecurity in Computer Science from George Washington University.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.