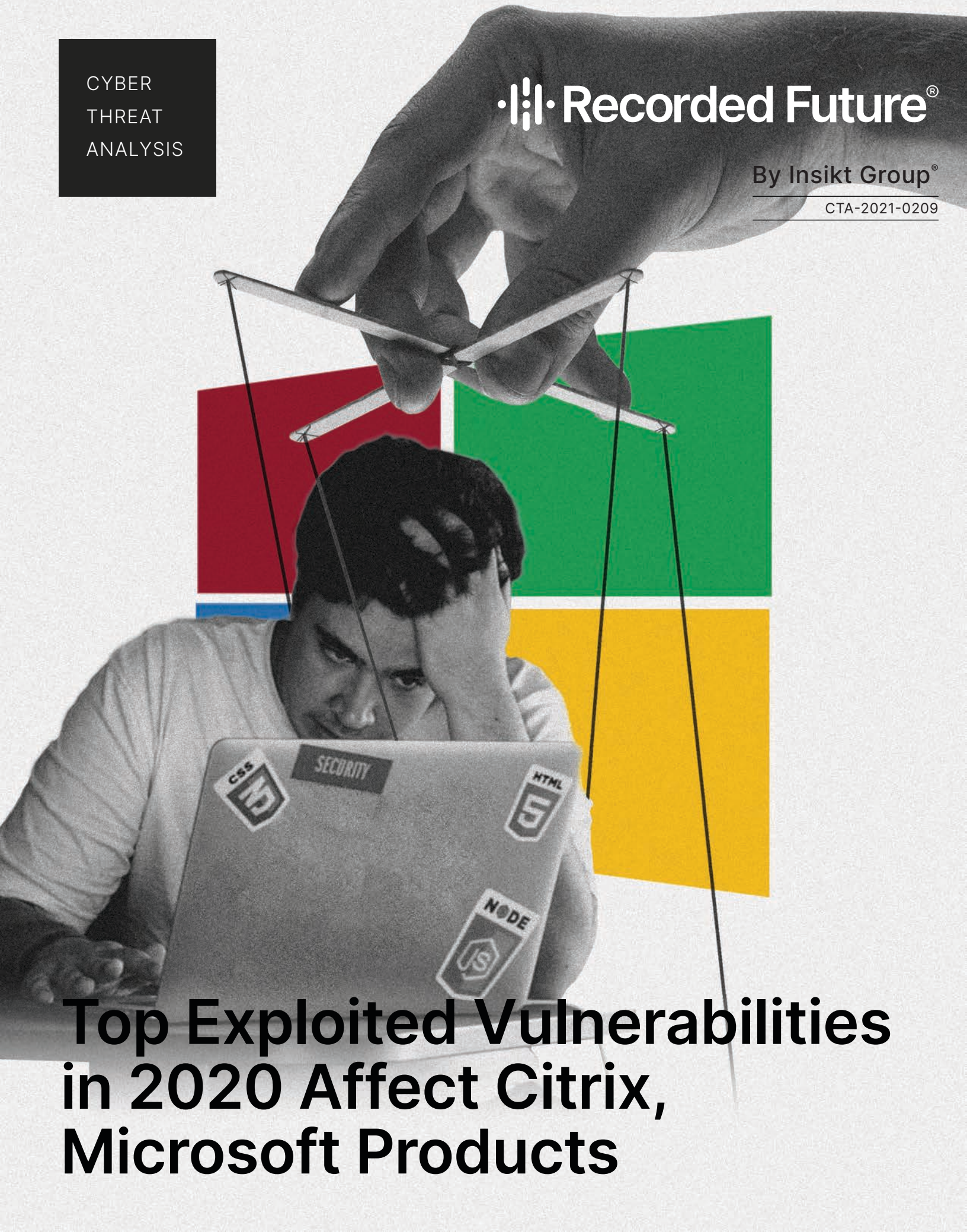


CYBER
THREAT
ANALYSIS


Recorded Future®

By Insikt Group®

CTA-2021-0209



Top Exploited Vulnerabilities in 2020 Affect Citrix, Microsoft Products



This analysis focuses on ransomware, exploit kit, phishing attack, or remote access trojan co-occurrences with vulnerabilities from January 1 to December 31, 2020. We analyzed thousands of sources, including code repositories, underground forum postings, and dark web sites. This is a follow-up to our [2019 report](#), and the intended audience includes information security practitioners, especially those supporting vulnerability risk assessments.

Executive Summary

This report highlights the top, most weaponized vulnerabilities in 2020 based on exploitation across all industries and associations with multiple types of malware. For the first time since this report's inception in 2015, no vulnerabilities in Adobe products make the list. This contrasts the first [report](#) published in 2015, where eight of the 10 top exploited vulnerabilities were Adobe products.

Similar to 2019, Recorded Future observed a majority of the top exploited vulnerabilities targeting Microsoft products (seven out of 10). One noticeable difference is that only one of these vulnerabilities targets Internet Explorer, compared to four in 2019. Also unique to 2020, the number of new vulnerabilities released initially [dropped](#) in March 2020 after the pandemic began. Ultimately, there were more than 18,000 new vulnerabilities identified in 2020.

Despite fewer overall vulnerabilities identified, the diversity of products impacted this year versus prior years stands out. The shift to working from home for employees globally opened up new avenues for exploitation against a homebound workforce. As such, products such as Citrix's Application Delivery Controller (ADC), PulseSecure's Pulse Connect, and Oracle's WebLogic appear on the list as targeted products for the first time.

The inclusion of more products on the list highlights that even official vulnerability databases and conventional scanning tools cannot arm organizations with one key metric: the overlap between the vulnerabilities in the systems you use and the ones that are being actively exploited by threat actors. Insight into weaponization is necessary to adequately prioritize vulnerabilities to patch, as often less than 1% of vulnerabilities have been weaponized within the past month or year. As such, it is imperative that security professionals know which vulnerabilities that impact a company's technology stack are included in exploit kits, used to distribute ransomware, a remote access trojan (RAT), or are currently being used in phishing attacks.

Key Judgments

- Seven of the top 10 vulnerabilities target Microsoft products, similar to 2019 and past reports.
- Only one CVE targeting Internet Explorer, CVE-2020-0674, is on the top 10 list, compared to four in 2019.
- There are no Adobe products included in the top targeted technologies, as Adobe Flash Player officially reached its end of life in December 2020.
- Citrix, PulseSecure and Oracle made their first appearances as targeted technologies in the annual top exploited list.
- Three of the top vulnerabilities were included in the top 10 of 2020 Patch Tuesday vulnerabilities: CVE-2020-1472, CVE-2020-0796 and CVE-2020-0674. The top exploited Patch Tuesday CVEs are also included in this report.
- Only two vulnerabilities were repeated from the 2019 top 10 list: CVE-2017-11882 and CVE-2012-0158. Both vulnerabilities were listed on the US-CERT's top 10 exploited vulnerabilities between 2016 to 2019.



The top three most **exploited vulnerabilities** in 2020 were:

Vulnerability	CVE-2019-19781
Company	Citrix
Product	Application Delivery Controller (ADC)
Associated Malware	Speculoos Backdoor, DoppelPaymer, Ragnar, Nefilim, Maze, Sodinokibi
CVSS SCORE	7.5
Vulnerability	CVE-2020-1472 (ZeroLogon)
Company	Microsoft
Product	Windows Server Process, Netlogon
Associated Malware	Ryuk, QuasarRAT
CVSS SCORE	9.3
Vulnerability	CVE-2019-11510
Company	PulseConnect
Product	Pulse Connect Secure (PCS) 8.2
Associated Malware	Sodinokibi, Black Kingdom
CVSS SCORE	7.5

TIPS

1

Prioritize patching Microsoft products — they are frequently exploited

Don't forget to patch older vulnerabilities — threat actors still use those

2

3

Use vulnerability intelligence to prioritize vulnerabilities exploited in the wild

Top Exploited Vulnerability Chart

Cyber Vulnerability	Company	Product	Associated Malware	CVSS	Recorded Future Risk Score
CVE-2019-19781	Citrix	Application Delivery Controller (ADC)	Speculoos Backdoor DoppelPaymer Ragnar Nefilim Maze Sodinokibi	7.5	89
CVE-2020-1472 (ZeroLogon)	Microsoft	Windows Server Process, Netlogon	Ryuk Ransomware QuasarRAT	9.3	99
CVE-2019-11510	PulseConnect	Pulse Connect Secure (PCS) 8.2	Sodinokibi Black Kingdom	7.5	79
CVE-2020-0796 (CoronaBlue, SMBGhost)	Microsoft	Windows Server 2016	Lemon Duck XMRig Miner	7.5	89
CVE-2017-11882	Microsoft	Office	Nanocore RAT Ramsay LCG EK LodaRAT	9.3	99
CVE-2020-0674	Microsoft	Internet Explorer	Gh0stRAT	7.6	99
CVE-2019-1367	Microsoft	Office	Magnitude EK Magniber Ransomware	7.6	99
CVE-2012-0158	Microsoft	Office	LimeRAT	9.3	99
CVE-2020-14882	Oracle	Web Logic Server	DarkIRC	10	79
CVE-2019-1458	Microsoft	Windows 10	Purple Fox EK Netwalker Ransomware	7.8	89

Table 1: The 10 most exploited vulnerabilities in 2020 (Source: Recorded Future)

Methodology

There was one change to the methodology in 2020: an additional data point, co-occurrences with ransomware. Recorded Future used a list of more than 4,000 strains of ransomware. Ransomware was added for a few reasons. First, the number of new exploit kits and exploit kit activity has continued to dwindle the past few [years](#). This decline is likely due to the ease in which a cybercriminal can purchase access directly to an organization instead of probing for vulnerabilities. Second, ransomware attacks have continued to increase, even more than possibly expected during the COVID-19 pandemic.

It is important to note that ransomware has a different “[kill chain](#)” compared to other malware strains. Ransomware can be distributed via a social engineering or weaponized website yet not activated for weeks or months. This means that a dropper malware, such as a RAT, may be used to install the ransomware on a victim's computer. For this reason, ransomware is often connected to other types of malware. For instance, a new [campaign](#) in November 2020 targeting German victims used the Gootkit trojan along with REvil ransomware.

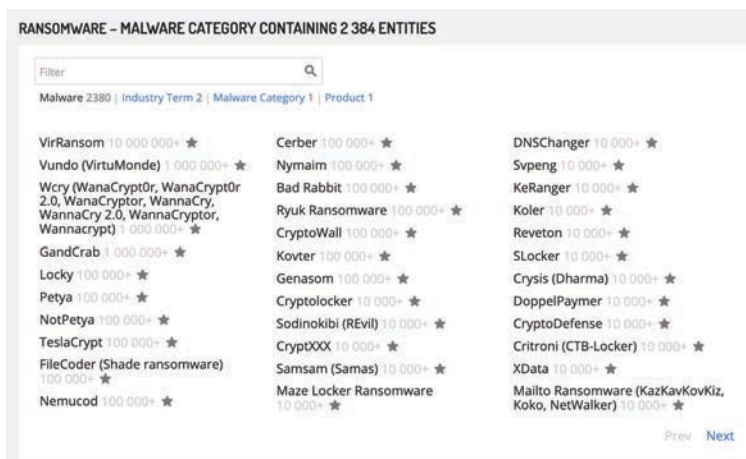


Figure 1: Ransomware category in Recorded Future

2020	2019	2018	2017	2016
1 .CVE2019-19781-	1 .CVE2018-15982-	1 .CVE2018-8174-	1 .CVE2017-0199-	1 .CVE2016-0189-
2 .CVE2020-1472-	2 .CVE2018-8174-	2 .CVE2018-4878-	2 .CVE2016-0189-	2 .CVE2016-1019-
3 .CVE2019-11510-	3 .CVE2017-11882-	3 .CVE2017-11882-	3 .CVE2017-0022-	3 .CVE2016-4117-
4 .CVE2020-0796-	4 .CVE2018-4878-	4 .CVE2017-8750-	4 .CVE2016-7200-	4 .CVE2015-8651-
5 .CVE2017-11882-	5 .CVE2019-0752-	5 .CVE2017-0199-	5 .CVE2016-7201-	5 .CVE2016-0034-
6 .CVE2020-0674-	6 .CVE2017-0199-	6 .CVE2016-0189-	6 .CVE2015-8651-	6 .CVE2016-1010-
7 .CVE2019-1367-	7 .CVE2015-2419-	7 .CVE2017-8570-	7 .CVE2014-6332-	7 .CVE2014-4113-
8 .CVE2012-0158-	8 .CVE2018-20250-	8 .CVE2018-8373-	8 .CVE2016-4117-	8 .CVE2015-8446-
9 .CVE2020-14882-	9 .CVE2017-8750-	9 .CVE2012-0158-	9 .CVE2016-1019-	9 .CVE2016-3298-
10 .CVE2019-1458-	10 .CVE2012-0158-	10 .CVE2015-1805-	10 .CVE2017-0037-	10 .CVE2015-7645-

Table 2: Top exploited CVEs between 2016 and 2020 (repeats are noted by color)

Using this updated methodology, there were only two repeated vulnerabilities from 2019 (there were six repeated vulnerabilities between the top exploited CVEs in both 2018 and 2019). The two repeated vulnerabilities between 2019 and 2020 are both listed in the US-CERT’s [publication](#) on the top exploited vulnerabilities between 2016 and 2019: CVE-2017-11882 and CVE-2012-0158. (The US-CERT’s report cited Recorded Future’s 2019 report.) There were only three repeated vulnerabilities that were not ransomware co-occurrences. Since prior years have had between five and six repeated vulnerabilities, this indicates that the trend for threat actors is towards exploiting a wider variety of products not before included in the top-exploited category.

As this annual list is based on both data and metadata analysis of available information from both open- and closed-source reporting, Recorded Future did not reverse-engineer any malware mentioned in this report. Instead, the aim of this report is to showcase the most exploited vulnerabilities.

Top Exploited Vulnerabilities

The top exploited vulnerability in 2020 was the Citrix Netscaler vulnerability CVE-2019-19781. This is the first appearance of this vulnerability in the report and the first Citrix product as the target of a top exploited vulnerability since this report first began in 2015. The vulnerability impacts Citrix Application Delivery Controller (ADC) and multiple Gateway versions between 10.5 and 13.0 to allow Directory Traversal. This CVE has been associated with various pieces of malware, including the Speculoos backdoor, deployed by the Chinese nation state APT41 to target various industries, such as healthcare, higher education, manufacturing and governments globally. Other nation-state threat actors, such as Iranian-affiliated Fox (also known as Pioneer Kitten), have targeted

institutions of interest via VPN technologies, including CVE-2019-19781. CVE-2019-19781 has also been associated with multiple types of ransomware families, including DoppelPaymer, RagnarLocker, Nefilim, Maze, and Sodinokibi.

The following timeline highlights the primary threat actors and malware this CVE was associated with in 2020.

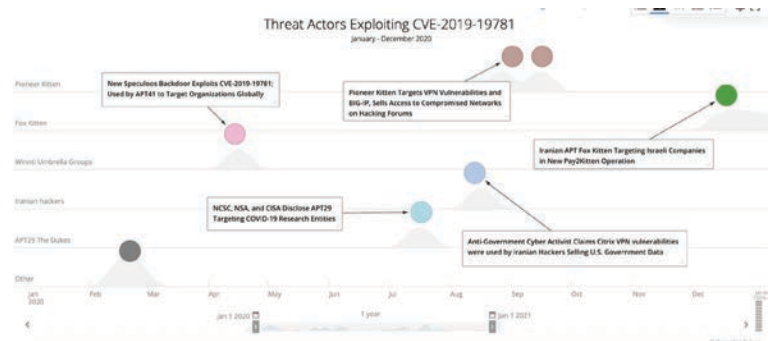


Figure 2: Timeline of exploitation of CVE-2019-19781 (Source: Recorded Future)

There were some dark web discussions about CVE-2019-19781 as well. In May 2020, a user named “Octoberine” claimed, in Russian, to have access to a “mountain of Citrix [targets] vulnerable to CVE-2019-19781”, where the user knew the LDAP passwords but was unsure where to go next.

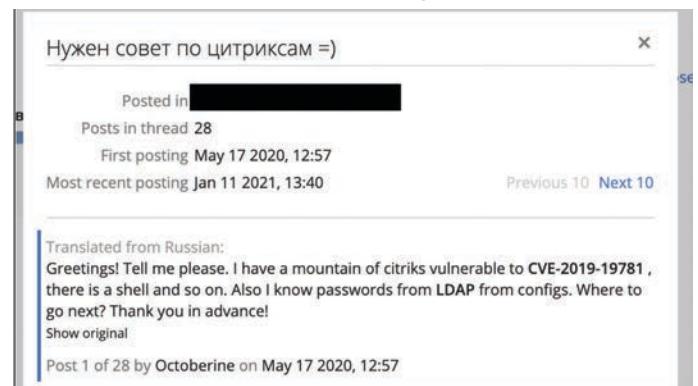


Figure 3: Dark web forum post requesting assistance exploiting CVE-2019-19781 (Source: Recorded Future)

CVE-2020-1472, or ZeroLogon, the second-highest risk vulnerability in this year's top 10, is a privilege escalation vulnerability that takes advantage of a weak cryptographic algorithm used in the Netlogon authentication process, and impacts Microsoft Windows domain controllers by Secura. It was reported by NIST on August 17, 2020, but not given more media attention until early to mid-September 2020. On October 6, 2020, it was identified that the vulnerability was [exploited](#) by Iranian nation-state threat actors for at least two weeks against unspecified targets. It is possible that media attention surged only a month after it was first reported on as a result of attackers developing and deploying exploits in the interim. The reverse situation could also be true: as ZeroLogon began to receive media attention, more and more attackers jumped on the possibility of exploitation. Either scenario could contribute greatly to ZeroLogon's quick and rapidly soaring popularity among cybercriminals this year. Insikt Group also observed six distinct proof-of-concepts (POCs) for the vulnerability on both open and closed sources.

Notable CVEs Published in 2020

More vulnerabilities that were first disclosed in 2020 made the year's top 10 list than comparably novel vulnerabilities in previous years. Within this top 10 list, four were disclosed in 2020, notably higher than only one in 2019 that was first disclosed that year but comparable to 2018's three. These four vulnerabilities were CVE-2020-1472 (ZeroLogon), CVE-2020-0796, CVE-2020-0674, and CVE-2020-14882. The first disclosed this year was CVE-2020-0674 in February 2020, with CVE-2020-0796 following in March 2020. ZeroLogon was initially disclosed by Microsoft in August 2020, and CVE-2020-14882 in October 2020.

One notable CVE first published in 2020 was CVE-2020-0796 (also known as CoronaBlue or SMBGhost), a remote code execution (RCE) vulnerability within the Microsoft Server Message Block 3.1 protocol. When first published, researchers noted that this vulnerability could have similar repercussions as a prior SMB vulnerability (SMBleed) that was exploited by WannaCry and NotPetya in 2017. In late October 2020, ThreatPost reported that there were still [103,000 vulnerable systems](#) accessible from the internet.

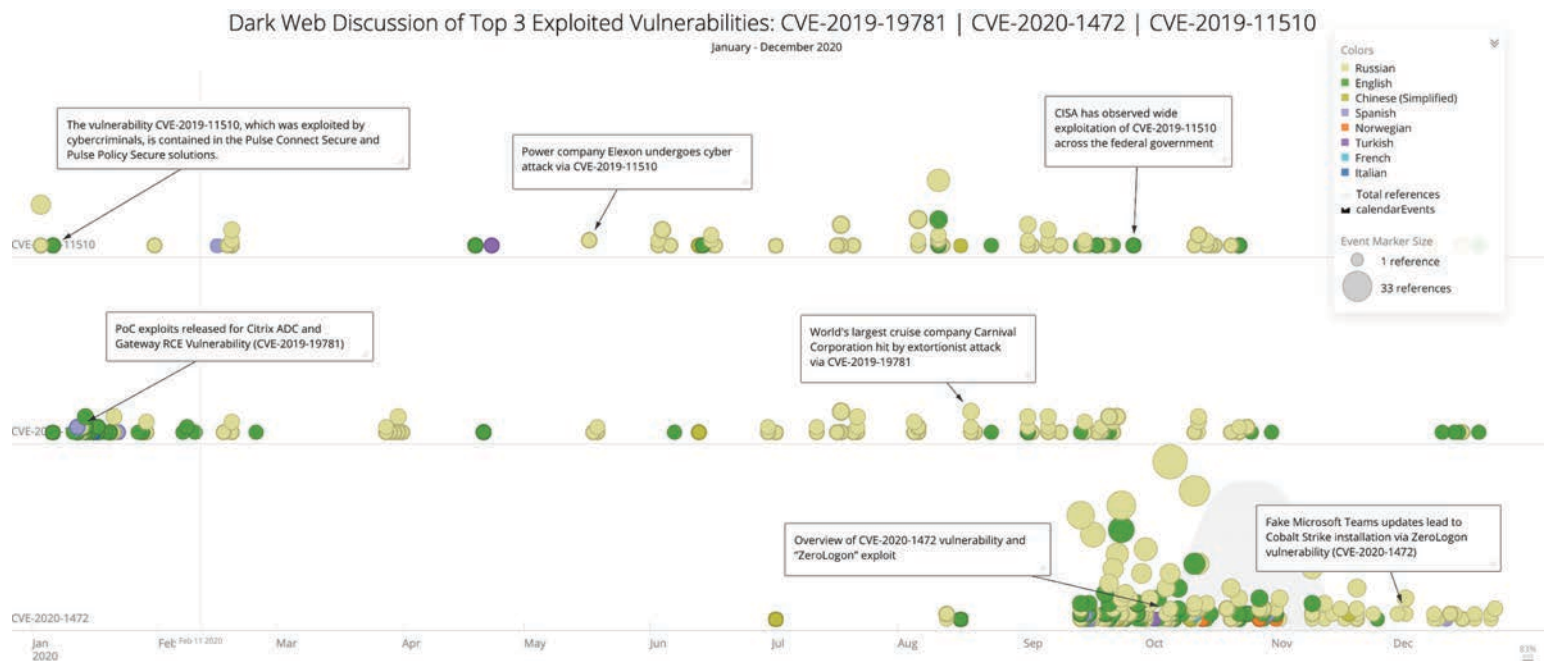


Figure 4: Timeline of dark web discussions of top three vulnerabilities (Source: Recorded Future)

This particular vulnerability had proof-of-concept code first published to GitHub in June 2020. Since then, the vulnerability has been associated with a new variant of the Lemon_Duck cryptomining malware used to infect Redis and Hadoop server instances. This new module option within Lemon_Duck malware allowed attackers to collect information on compromised machines. The spike in Lemon_Duck infections was likely due to the threat actors' use of COVID-19-themed phishing emails, which used XMRig miner as a deployment mechanism to install Lemon_Duck. As recently as December 2020, a user on one dark web forum was requesting assistance with finding exploits related to SMBGhost (and BlueKeep).

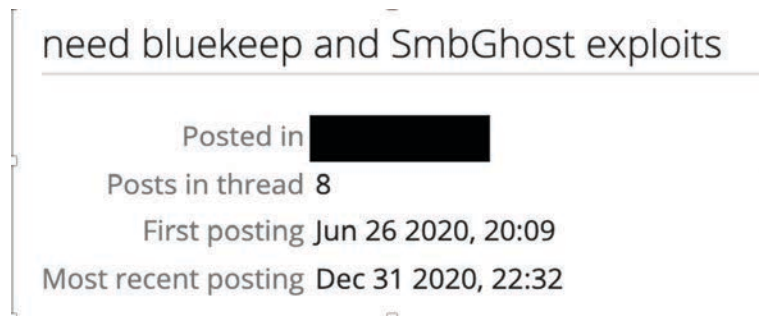


Figure 5: Dark web forum post requesting SMBGhost and BlueKeep exploits

Another notable 2020 vulnerability that made it on the list was CVE-2020-0674. First disclosed in an out-of-band [security advisory](#) by Microsoft in January 2020 and confirmed [exploited](#) in the [wild](#) before a patch was released in February 2020, CVE-2020-0674 is a critical scripting engine memory corruption vulnerability in Internet Explorer that allows attackers to execute arbitrary code in the context of the current user. Insikt Group has observed multiple instances of proof-of-concept code exploiting this vulnerability. While this vulnerability does not pose too substantial a threat in corporate networks as most organizations have migrated away from Internet Explorer, it [continues to be widely exploited](#), especially by Purple Fox.

Top Patch Tuesday CVEs in 2020

Prior to December 2020's Patch Tuesday release, Microsoft had announced 1,198 total vulnerabilities in 2020, an average of almost 109 vulnerabilities per month. Compare this to 800 vulnerabilities disclosed in all of 2019, an average of just over 66 per month.

The following chart ranks the vulnerabilities with the highest degree of exploitation that were released by Microsoft in 2020. Most of the vulnerabilities were released in the early part of 2020.

CVE	Description	Month Released	Recorded Future Risk Score
CVE-2020-0674	Scripting Engine Memory Corruption Vulnerability	February	99
CVE-2020-1472 (ZeroLogon)	Netlogon Elevation of Privilege Vulnerability	August	89
CVE-2020-0796 (SMBGhost)	Windows SMBv3 Client/Server Remote Code Execution Vulnerability	March	89
CVE-2020-1350 (SIGRed)	Windows DNS Server Remote Code Execution Vulnerability	July	89
CVE-2020-0601 (CurveBall)	Windows CryptoAPI Spoofing Vulnerability	January	89
CVE-2020-0688	Microsoft Exchange Memory Corruption Vulnerability	February	89
CVE-2020-1147	.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability	July	89
CVE-2020-0787	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability	March	89
CVE-2020-0668	Windows Kernel Elevation of Privilege Vulnerability	February	89
CVE-2020-0683	Windows Installer Elevation of Privilege Vulnerability	February	89
CVE-2020-0938	Adobe Font Manager Library Remote Code Execution Vulnerability	April	89
CVE-2020-1362	Windows WalletService Elevation of Privilege Vulnerability	July	89

Table 3: Top CVEs released in Patch Tuesday updates in 2020

New Product Additions to Targeted List

One of the newer vulnerabilities on this list was CVE-2019-11510. First disclosed in May 2019, CVE-2019-11510 allows unauthenticated attackers to send specially crafted URLs to connect to vulnerable Pulse Secure servers. Although a patch was released the same month, CISA advised organizations in April 2020 to update all Active Directory passwords as they observed credentials used months after organizations had patched against this vulnerability.

The vulnerability was observed actively exploited in the wild by Iranian nation-state threat actors on multiple occasions throughout 2020 including in [February 2020](#) and [September 2020](#). CVE 2019-11510 has been associated with a new ransomware variant called Black Kingdom, which was first observed in February 2020.

Top Tested Vulnerabilities

Two of the top vulnerabilities, CVE-2017-11882 and CVE-2019-1367, were two of the 10 most commonly tested vulnerabilities per VirusTotal uploads according to a November Recorded Future [report](#). CVE-2017-11882, a Microsoft Office vulnerability, which can allow an attacker to execute arbitrary code via a crafted document, is associated with the Nanocore RAT, whose source code is publicly available. CVE-2017-11882 is also associated with a new ransomware strain dubbed [Ramsay](#) that was designed to infect air-gapped networks. CVE-2017-11882 was also on the top exploited vulnerability list in 2018 and 2019 at the number three spot, respectively.

Vulnerability-Specific Patches

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

CVE	Remediation	Recorded Future Risk Score
CVE-2019-19781	The administrator will need to login to the ADC instance using these credentials to apply the mitigations. The full steps are included at: https://support.citrix.com/article/CTX267679	89
CVE-2020-1472 (ZeroLogon)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472	99
CVE-2019-11510	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/	89
CVE-2020-0796 (CoronaBlue)	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796	89
CVE-2017-11882	Update affected Microsoft products with the latest security patches: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882	99
CVE-2020-0674	https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674	99
CVE-2019-1367	https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367	99
CVE-2012-0158	Update affected Microsoft products with the latest security patches: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-027	99
CVE-2020-14882	https://www.oracle.com/security-alerts/cpuoct2020.html	99
CVE-2019-1458	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-1458	89

Table 4: Remediations for top vulnerabilities of 2020

Recommended Actions

The goal of this annual list is to provide an account of the most widely adopted vulnerability exploits by the cybercriminal underground. Security teams can take action on data within this report with any of the following recommended actions:

- Given the outsized number of exploits included in this top exploited list, prioritize the patching of Microsoft products in your technology stack.
- Prioritize patching of all the vulnerabilities identified in this report.
- Do not forget to patch older vulnerabilities — the average vulnerability stays alive for nearly seven years, according to a 2017 RAND [report](#). Recently disclosed vulnerabilities are not the only software targeted by threat actors.
- Remove affected software if it does not impact key business processes.
- Install browser ad-blockers to prevent exploitation via malvertising.
- Frequently back up systems, particularly those with shared files, which are regular ransomware targets.
- Conduct or maintain phishing security awareness to mitigate attacks. This can include user training to encourage skepticism of emails requesting additional information or prompting clicks on any links or attachments. Companies will not generally ask customers for personal or financial data, but when in doubt, contact the company directly by phone and confirm if they actually need the information.
- Vulnerability management teams can use Recorded Future's technical intelligence to prioritize patching based on which vulnerabilities are actively being exploited in the wild by malware.

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 hundreds of businesses and government organizations around the world.