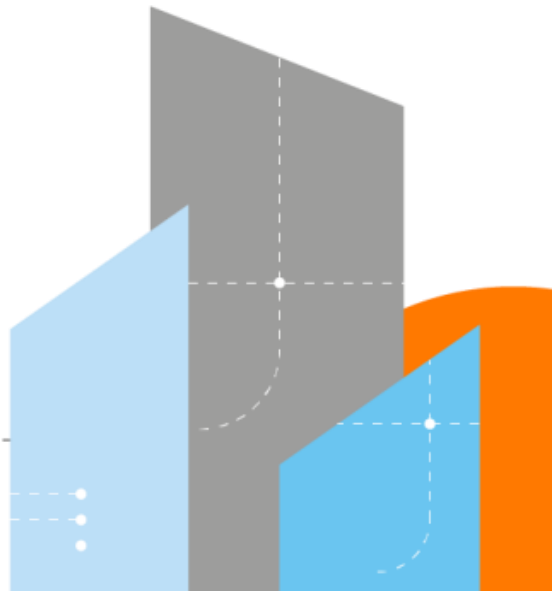
Orange
Cyberdefense

Security Intelligence

Monthly Report

November 2022



CONTENTS

INTRODUCTION

Welcome to our last monthly report of 2022, hot on the heels of our Security Navigator report, which is now available to download, see the details in the “At a glance” cutout.

Here’s hoping for a quiet last couple of weeks of the year, although given events in recent years we won’t be counting our chickens just yet!!

This month we have a guest contributor to the Editor’s Note section. The current excitement surrounding the ChatGPT artificial intelligence driven service got to us too. We decided to ask ChatGPT about cyber security and to make some predictions about future cyber threats.

On behalf of the Security Research Center team and everyone at Orange Cyberdefense we hope you all have a Merry Christmas and a Happy New Year!!

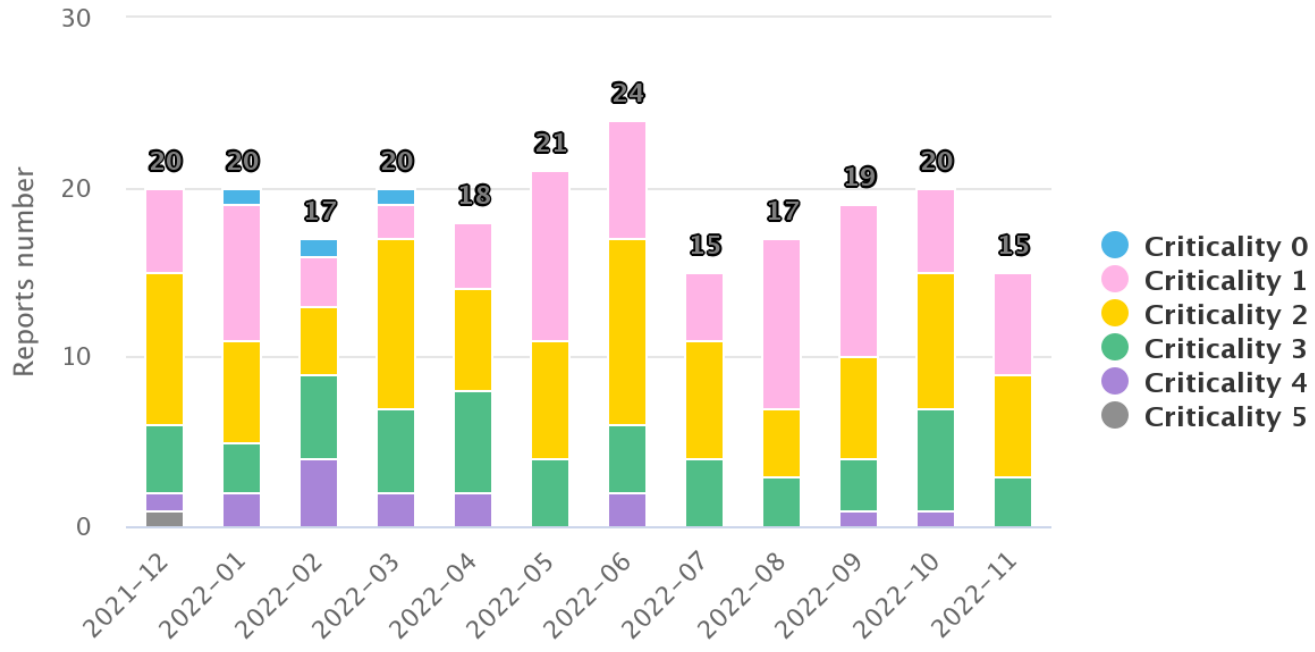
At a glance

Our new 2023 Security Navigator report offers 120+ pages full of invaluable, unique and comprehensive insights, backed up by in-depth analysis of #MDR data, malware trends, and attack patterns observed for different industries and business sizes. Curious?

Get your copy today:
http://ow.ly/kx6050LVfaA

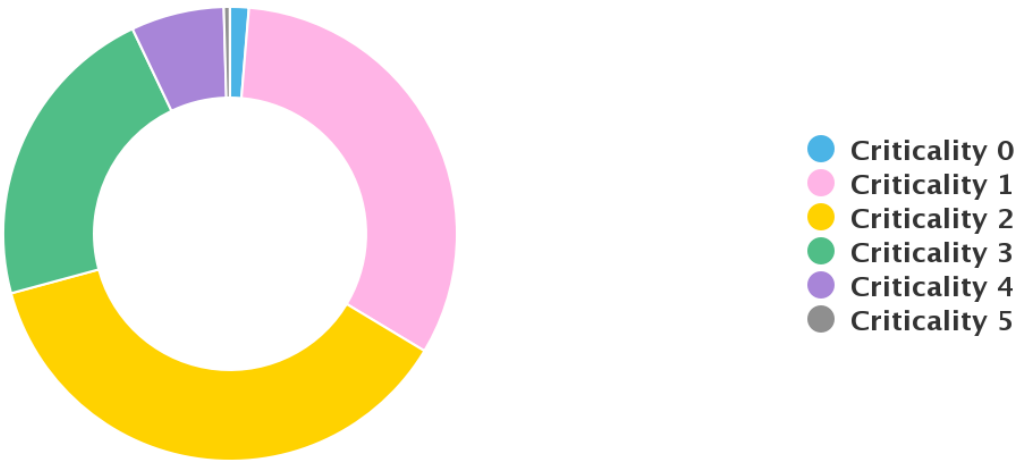
World Watch Review November 2022

The Orange Cyberdefense CERT published a total of 15 new World Watch advisories during November 2022, along with adding updates to a further 22 previously published advisories. This volume of new advisories represents a slight dip compared to the previous 3 months; however, this is likely caused by a decline in activity generally, potentially due to the upcoming holiday period.



Breakdown of Published Advisories Previous 12 Months

Alongside the lower number of advisories, the criticality levels allocated to the November advisories again remained low. The highest allocated criticality was level 3, with only three of these being published this month.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As can be seen above the advisories this month were all given criticality ratings of low or medium when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring, however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

SIG-662179 - PLAY ransomware now publishes victims on their new data leak site

- Since last September, when we first covered the PLAY ransomware here (as a rebrand from the Hive and/or Nokoyawa group), the gang has been very active, targeting dozens of organizations from Europe, North and South America, and Asia. Recently, Orange Cyberdefense handled one incident involving this new ransomware group, giving us some insights on the group's malware and techniques.
- The PLAY ransomware gang also hosts a data leak site available through Tor since a few weeks, thus many of their past victims are now known. However they still hide the names of some of the recent victims, in a trending attempt to force them to pay the ransom in order to prevent their name to be revealed.

SIG-657053 - High severity vulnerability in OpenSSL but affecting only version 3.x

- The OpenSSL project team announced on October 26th that they would release on November 1st a new version of the OpenSSL library, to fix a CRITICAL security issue in the 3.0.x branch only. And OpenSSL provided indeed yesterday at 3pm UTC an advisory but with a downgraded severity level, for two joined vulnerabilities considered only as HIGH risk. They also as expected released the new version numbered 3.0.7, fixing together 2 CVEs numbered: CVE-2022-3786 and CVE-2022-3602.
- Fortunately, this vulnerability does not affect OpenSSL versions prior to 3.x, and in particular the most currently used one: version 1.1.1. Thus, the overall risk is greatly reduced, as this latest 3.x version launched a year ago is almost never used in applications curently embedding OpenSSL. Only a few thousands exposed assets identified by passive scanners are currently considered vulnerables, whereas millions are curently using the v1.x branch.
- Finally, the risk associated involves an easy Denial of Service with a specially crafted X.509 certificate, but Remote Code Execution is mostly theoretical and yet unproven, as way more complex to achieve. PoC codes to achieve this DoS behavior are nevertheless already publicly available, but no massive attack attempts are currently recorded yet. The malicious certificates needed must be signed by a Certificate Authority as the issue happens after certificate validation.
- OpenSSL forks such as LibreSSL (used by default on macOS) or BoringSSL (in Chrome) confirmed not being impacted, as so did some vendors such as JFrog. Only a handful of Linux distributions currently embed the vulnerable OpenSSL version, including RHEL 9, Debian 12, Fedora 36 or Ubuntu 22.04. A list of vulnerable applications is available on the Dutch National CERT's GitHub page.

SIG-661617 - Sophos and McAfee engines in Cisco Secure Email Gateways can be circumvented

- On November 14, an anonymous researcher publicly disclosed three different methods to bypass some of the antivirus engines in Cisco Secure Email Gateway (formerly known as IronPort) appliance and deliver malware using such specially crafted emails. Indeed, detection can be circumvented by a remote attacker that leverages error tolerance and different Multipurpose Internet Mail Extensions (MIME) decoding capabilities of email clients. The attack complexity is very low and working exploits have already been disclosed. It is also worth mentioning that it impacts devices running with a default configuration.
- Cisco said it was aware of an issue impacting only at this point the Sophos and McAfee scanning engines embedded in Cisco Secure Email Gateway and has released a workaround for its users. However, the issue will likely not be directly fixed by the vendor as it is not considered a vulnerability.

Editor's Notes

Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Wicus

In pursuit of more secure systems

The U.S. Cybersecurity and Infrastructure Security Agency or CISA keeps a catalog of vulnerabilities that are known to be exploited and is officially referred to as the Known Exploited Vulnerabilities (KEV) Catalog. All U.S. Federal agencies must track the KEV Catalog and any product listed on it must be patched by the required date. The KEV Catalog is freely available for download and contained 860 vulnerability entries at the time of writing and is indexed using the CVE ID.

Similarly, a group consisting of CSW, Securin, Cyware, and Ivanti published analysis on vulnerabilities being used by attackers related to ransomware incidents titled 'Ransomware Through the Lens of Threat and Vulnerability Management Index Update Q2 – Q3 2022'. Included in the report is a Ransomware Index that shows that the number of vulnerabilities exploited grew from 310 in Q1 2022 to 323 in Q3 2022. The table from Appendix B is particularly interesting as it contains the Top 10 most exploited vulnerabilities and is listed here:

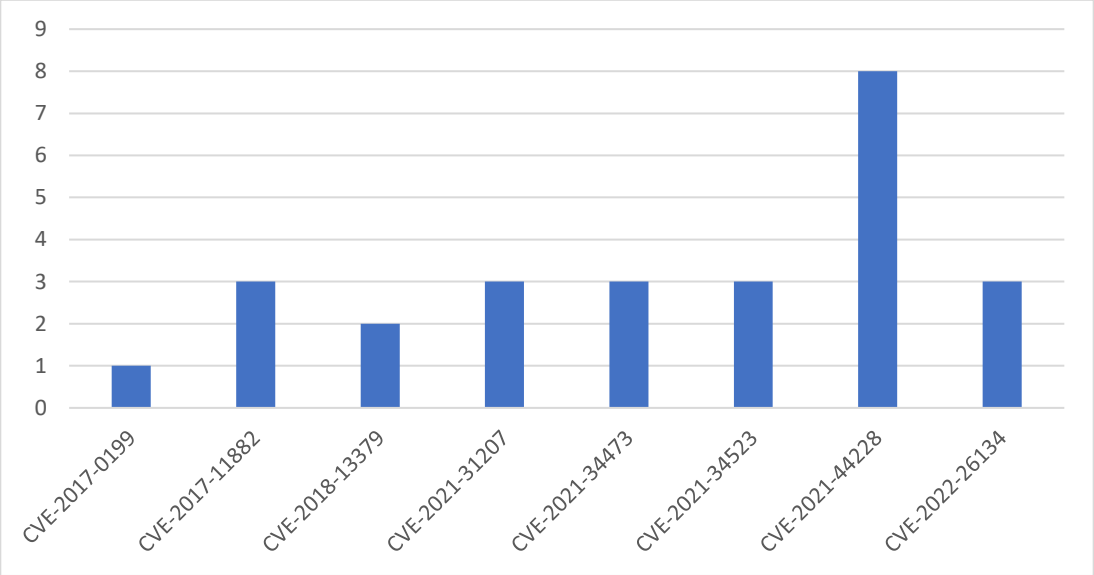
CVE	Vendor	Product
CVE-2021-44228	Log4J	175 products
CVE-2022-26134	Atlassian	3 products
CVE-2021-31207	Microsoft	Exchange Server
CVE-2021-34473	Microsoft	Exchange Server
CVE-2021-34523	Microsoft	Exchange Server
CVE-2020-5902	F5	16 products
CVE-2018-8174	Microsoft	10 products
CVE-2018-13379	Fortinet	FortiOS
CVE-2017-0199	Microsoft	13 products
CVE-2017-11882	Microsoft	Office

It is not clear how this Top 10 was calculated, but it is unsurprising that the Log4J vulnerability, tracked as CVE-2021-44228, features prominently.

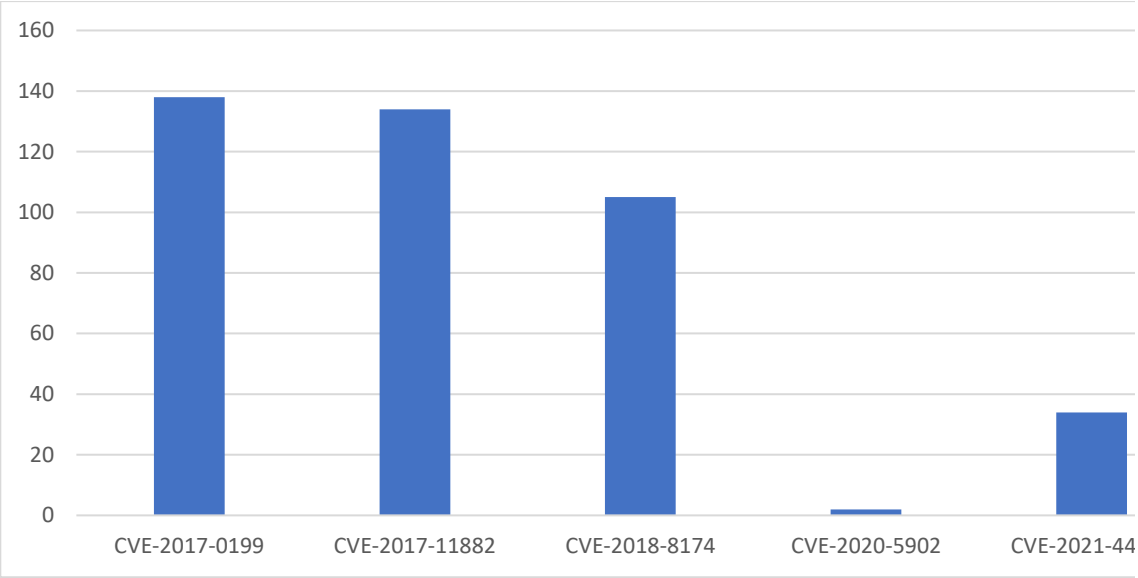
We took our own datasets, namely the VSOC scanning data, Penetration Testing, and World Watch Advisories to determine the extent the Ransomware Index Top 10 and the KEV Catalog features in what we observe and report.

Comparing the Top 10 with the World Watch Advisories we see that we covered 8 of the 10 during the period October 2021 up to and including September 2022. The vulnerabilities not covered by our World Watch Advisories are CVE-2020-5902, a remote code execution vulnerability in the Traffic Management User Interface (TMUI) of F5 BIG-IP, and a remote code execution vulnerability in the Microsoft VBScript Engine, tracked as CVE-2018-8174. The absence of these two vulnerabilities is simply due to not publishing any advisories containing explicit reference to these vulnerabilities.

The Log4J vulnerability, CVE-2021-44228, was mentioned the most during the period compared to the other vulnerabilities. The Log4J flaw was at the time considered a very serious flaw due to the impact it could have had. Security professionals were convinced that this flaw, if left unpatched, could result in devastating breaches. When examining the relevant World Watch Advisories that mentions the vulnerabilities present in the chart, we can see the context matches the exploitation theme of the Ransomware Index Top 10 as well as vulnerability management for flaws discovered during the period considered.



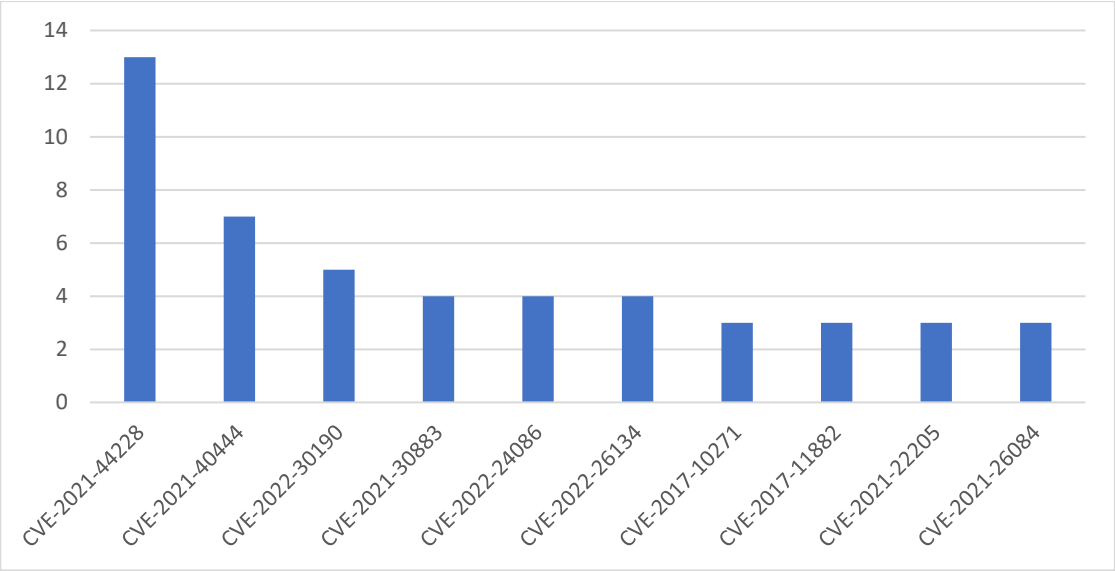
The picture is slightly different when looking at the occurrence of the Ransomware Index Top 10 in terms of the VSOC scanning data. The two vulnerabilities, CVE-2020-5902 and CVE-2018-8174, that were absent when compared with the Top 10 and the World Watch Advisories are present in this set, but we only see 5 of the possible 10 vulnerabilities in the assets scanned. The three prominent CVEs here are all related to Microsoft products where CVE-2017-0199 and CVE-2017-11882 impact Microsoft Office 2007 through 2016. Vulnerability CVE-2018-8174, as mentioned earlier, impacts the VBScript Engine. One could speculate that these three vulnerabilities are exploited through phishing emails with malicious attachments or links to malicious office documents. The Log4J vulnerability, CVE-2021-44228 is present to no surprise, but to lesser extent. Our VSOC team also identified 2 F5 BIG-IP TMUI assets impacted by CVE-2020-5902.



Intersecting the Top 10 vulnerabilities from the Ransomware Index and vulnerabilities reported by our Ethical Hacking team during assessments we only find the Log4J vulnerability, CVE-2021-44228. This might seem odd as one might think that Penetration Testing is supposed to highlight common vulnerabilities, but that would be a costly mistake. Penetration Testing must not equate to vulnerability scanning and any consultancy worth their weight in gold will tell you that. Penetration Testing should be scoped to identify flaws that cannot be identified by vulnerability scanners, such as flaws in APIs, programming errors in applications, excessive permissions, configuration flaws, etc. Some vulnerabilities do lend itself naturally to fit in with actions performed by ethical hacking teams, but these vulnerabilities could also be identified using scanning.

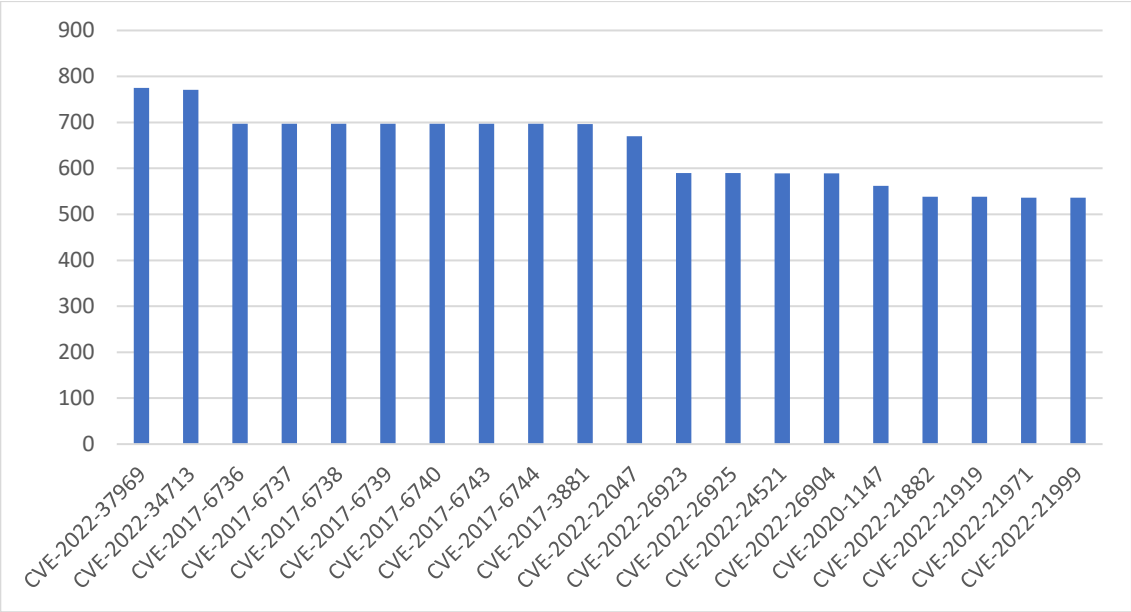
When comparing vulnerabilities mentioned in the World Watch Advisories, VSOC scanning data, and Penetration Testing data with the KEV Catalog we see a slightly different story, but with familiar elements. Also, bear in mind that the KEV Catalog has 860 entries at the time of writing, so we are sampling across a much larger set.

Comparing the vulnerabilities mentioned in the World Watch Advisories with the KEV Catalog we see that the first 10 vulnerabilities here:



The Top 10 vulnerabilities of the Ransomware Index are a subset of the KEV Catalog, and it would be expected to see the vulnerabilities we saw earlier here. Bear in mind this chart is limited to the first 10 records and is ordered according to the number of appearances of the CVE as well as ordered by the CVE value from oldest to newest. The Log4J vulnerability is still present here and this means that it was the most prominent vulnerability in our World Watch Advisories for the period October 2021 up to and including September 2022. We also observed vulnerabilities CVE-2017-11882, Microsoft Office, and CVE-2022-26134, Atlassian Confluence. The second highest number of mentions goes to a remote code execution vulnerability impacting Microsoft MSHTML and is tracked as CVE-2021-40444 and this was not present in the Top 10 of the Ransomware Index. The third most mentioned vulnerability impacts the Microsoft Windows Support Diagnostics Tool (MSDT) and is tracked as CVE-2022-30190.

When cross referencing the VSOC scanning data with the KEV Catalog we see a rather different picture. Once again bear in mind that the KEV Catalog contains 860 entries. Microsoft vulnerabilities dominate the first 20 records evaluated as pictured below. We did observe a large chunk of CISCO IOS vulnerabilities relating to an SNMP flaw in the assets we scanned.

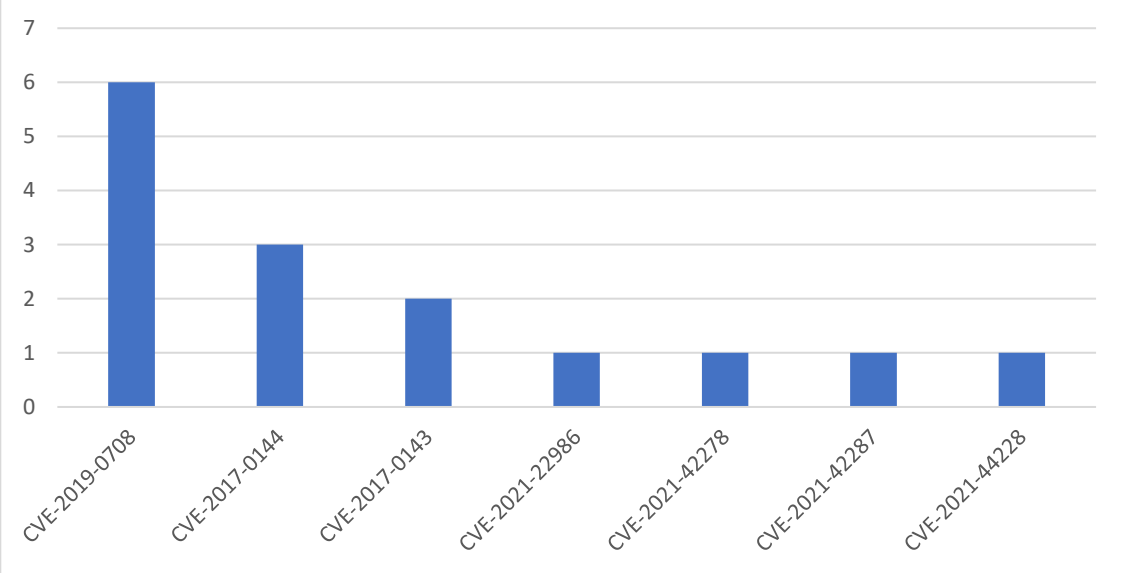


The table lists the descriptions of the relevant vulnerabilities related to the chart VSOC/KEV Catalog chart.

CVE	Impact
CVE-2022-37969	Windows Common Log File System Driver
CVE-2022-34713	Microsoft Windows Support Diagnostic Tool (MSDT)
CVE-2017-6736	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6737	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6738	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6739	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6740	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6743	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-6744	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS
CVE-2017-3881	Cisco IOS and Cisco IOS XE
CVE-2022-22047	Windows CSRSS
CVE-2022-26923	Active Directory Domain Services
CVE-2022-26925	Windows LSA
CVE-2022-24521	Windows Common Log File System
CVE-2022-26904	Windows User Profile
CVE-2020-1147	NET Framework, SharePoint Server, and Visual Studio

CVE-2022-21882	Windows and Windows Server
CVE-2022-21919	Windows User Profile Service
CVE-2022-21971	Windows
CVE-2022-21999	Windows Print Spooler

Comparing the vulnerabilities observed in the penetration testing dataset with the KEV Catalog we observe a data set that illustrates the type of low hanging fruit ethical hackers or real attackers will first try to exploit. These vulnerabilities can be targeted using reliable exploits from the public domain that anyone can use to breach a vulnerable system. All these vulnerabilities can be detected using automated scanning, but these vulnerabilities are so easy to exploit, and it makes sense for ethical hackers to probe these to demonstrate how a likely adversary could compromise the vulnerable system in scope.



CVE	Impact
CVE-2019-0708	Microsoft Remote Desktop Protocol
CVE-2017-0144	Microsoft Windows SMB
CVE-2017-0143	Microsoft Windows SMB
CVE-2021-22986	F5 BIG-IP
CVE-2021-42278	Microsoft Server Active Directory
CVE-2021-42287	Microsoft Server Active Directory
CVE-2021-44228	Log4J

What does all this mean? One could be philosophical about this by saying ‘Knowing is half the battle’, but the real battle is putting plans into action to mitigate or resolve impacted systems. The success of a good security plan is to know how to get the most out of limited budgets and doing so with few well-trained staff. Focusing on vulnerabilities that are often targeted can help you buy time as this can fend off opportunistic attacks. Effectively defending against persistent attacks is hard work and requires constant evaluation of your environment. Knowing what is critical to your organization will help you determine where to focus extra effort when engaging in vulnerability scanning services or contracting ethical hackers.

ChatGPT

Guest Talk

Hello, I am ChatGPT, a large language model trained by OpenAI. I am designed to assist with a variety of tasks, including answering questions and providing information on a wide range of topics. I am constantly learning and improving, and I am here to help with whatever is need. Today I will talk about why Security is so important and where I think the future lies.

Security is critical because it helps to ensure the integrity and reliability of information and systems. In the modern world, we rely heavily on technology for everything from communication and financial transactions to the control of critical infrastructure. If these systems are not secure, it can have serious consequences such as financial loss, loss of sensitive information, or even disruption of essential services. Ensuring the security of these systems is essential to maintaining the reliability and trustworthiness of the information and services they provide. some of the most common and prominent threats include malware, ransomware, phishing attacks, and distributed denial of service (DDoS) attacks.

There are several best practices that businesses can follow to improve their cyber security. These include:

1. Implementing strong and unique passwords for all accounts and regularly updating them.
2. Ensuring that all software and applications are kept up to date with the latest security patches.
3. Using firewalls and other security technologies to protect networks and systems from external threats.
4. Implementing secure protocols for communication and data transfer, such as HTTPS and VPNs.
5. Providing regular security training to employees to help them identify and avoid potential threats.
6. Conducting regular security audits and assessments to identify and address vulnerabilities.
7. Developing a comprehensive security plan and incident response plan in case of a security breach.

By implementing these practices, businesses can greatly reduce their risk of falling victim to cyber threats and protect sensitive data and systems.

It is difficult to predict the future of cyber security threats with certainty, as the threat landscape is constantly evolving, and new threats are constantly emerging. However, it is likely that the future will see an increase in the use of artificial intelligence (AI) and machine learning by both attackers and defenders.

On the one hand, AI and machine learning can be used to automate and improve the effectiveness of cyber-attacks. For example, attackers may use AI to automate the process of discovering and exploiting vulnerabilities, or to create more sophisticated and convincing phishing emails.

On the other hand, AI and machine learning can also be used to improve the ability of defenders to detect and respond to cyber threats. For example, machine learning algorithms can be trained to recognize patterns in network traffic or email content that indicate the presence of a threat and can take automated actions to defend against the threat.

Overall, the future of cyber security is likely to involve a continuous arms race between attackers and defenders, with both sides using increasingly advanced technologies to gain the upper hand.

https://openai.com/

Good News Cyber

Google has released a set of open-source detection rules to find versions of Cobalt Strike that are being misused by malicious actors. Whilst Cobalt Strike is a legitimate commercial penetration testing tool it is often abused by malicious actors who bypass the vetting process by using older leaked or cracked versions of the software. By developing detection signatures for older versions Google hopes to make Cobalt Strike harder to misuse and "move the tool back to the domain of legitimate red teams". The YARA rules can be found here: https://github.com/chronicle/GCTI

INTERPOL announced a five-month long international operation involving fraud investigators around the world had resulted in the arrest of nearly 1000 suspects and the seizure of USD$130m in virtual assets. The operation targeted "voice phishing, romance scams, sextortion, investment fraud and money laundering associated with illegal online gambling".

iSpoof, a service that allowed users to make calls and send SMS messages using spoofed identities has had its servers and websites seized by Europol and other law enforcement agencies from several countries. Launched in December 2020 the service marketed itself as a way for users to protect their phone numbers and identities online, but instead iSpoof became widely abused for fraud allowing cybercrime gangs to pose as banks and other financial organizations. According to Europol iSpoof was being used to place more than one million spoofed calls every month, its administrators made more than €3.7 million, and that the service has been linked to fraud and losses of over €115 million worldwide.