BRISK INFOSEC

CYBER TRUST & ASSURANCE

EDITION 41

THREATSPLOIT

ADVERSARY REPORT

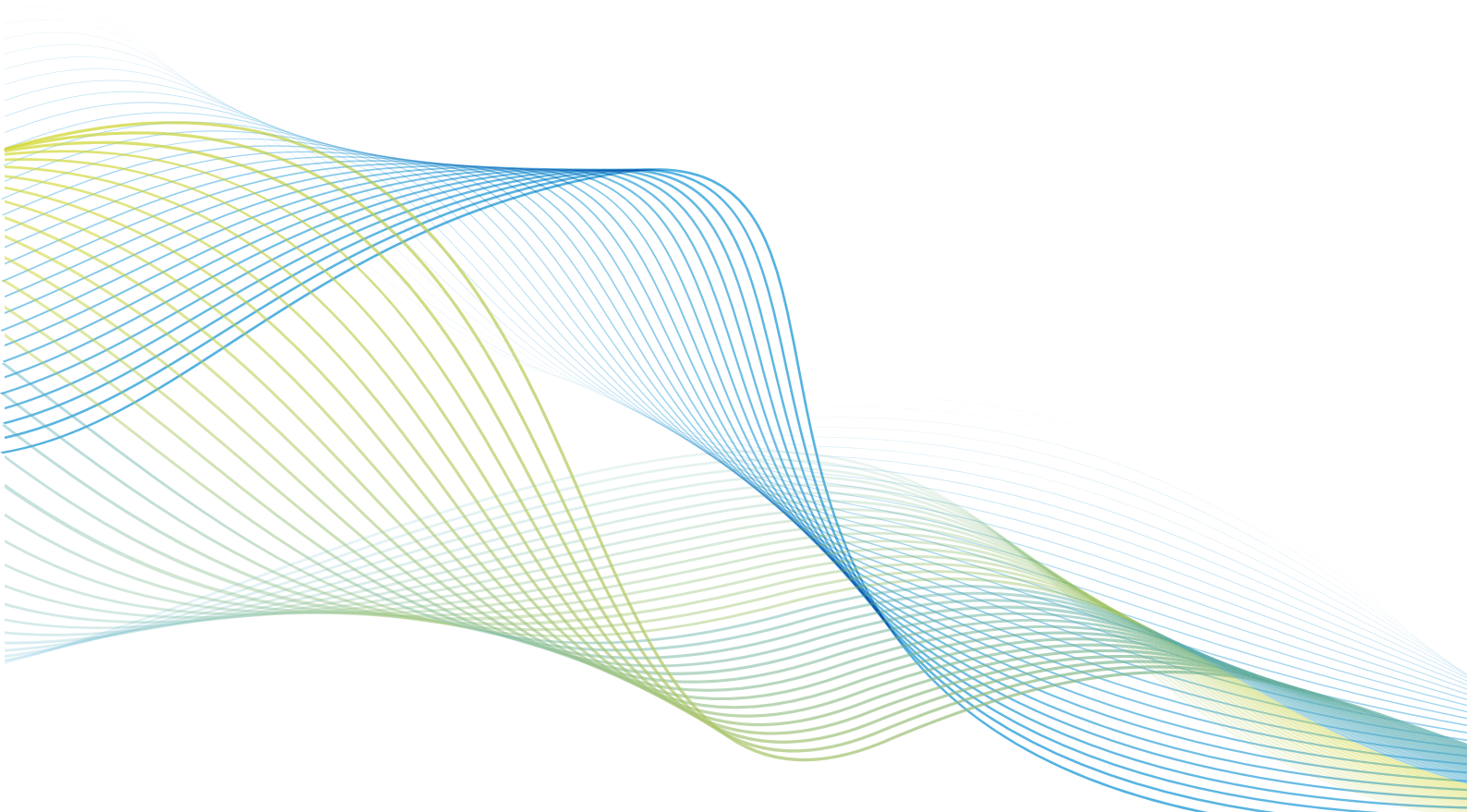
INTRODUCTION

Welcome to the Threatsploit Report of january 2022 covering some of the important cybersecurity events, incidents and exploits that occurred this month. This month, the cybersecurity sector witnessed a massive rise in ransomware and data breach attacks across geographies. Besides, many other attack types were seen spiking during these recent months.

The primary reason is and has always been the same….

”EMPLOYEES AND STAKEHOLDERS HAVE LIMITED OR NO PERCEPTION OR UNDERSTANDING OF THREATS AND MISPLACED UNDERSTANDING OF MASSIVE CYBER THREATS OR CONSEQUENCES”.

Since the time Work From Home (WFH) has become the new normal, security incidents has peaked with more and more issues relating to VPNs and other remote connecting mediums. WFH option has further limited the ability of IT functions to apply software patches for both old and new critical vulnerabilities, exposing the information assets for hackers to exploit and compromise. Let us walk you through some of the important security incidents that happened this month.



CONTENTS

‘LOG4SHELL’ VULNERABILITY POSES CRITICAL THREAT TO APPLICATIONS USING ‘UBIQUITOUS’ JAVA LOGGING PACKAGE APACHE LOG4J

The maintainers of popular Java logging library Apache Log4j have rushed out a patch for a critical vulnerability that could lead to remote code execution (RCE) in numerous applications. The relative ease of exploitation, attackers’ ability to seize control of targeted servers, and the ubiquity of Log4j make for a serious situation. Dubbed ‘Log4Shell’ and credited to Chen Zhaojun of Alibaba, the vulnerability (CVE-2021-44228) has been assigned the maximum CVSS score of 10. The scope of affected applications is comparable to the 2015 commons-collection vulnerability (CVE 2015-7501) because attackers can safely assume targets likely have this on the classpath. It has been documented that various exploits and other key information about the vulnerability in a blog post published yesterday (December 9) and are still posting updates as fresh details emerge. Servers are vulnerable if they are running a vulnerable Log4j version and have an endpoint protocol that allows an attacker to send an exploit string and log statement that logs out the string from the request, they said. Apache Log4j2 versions 2.14.1 and below fail to protect against attacker-controlled (Lightweight Directory Access Protocol) (LDAP) and other JNDI-related endpoints, according to the CVE description. “An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled,” it says. This behavior is no longer enabled by default in Log4j 2.15.0 and “users are strongly discouraged from enabling it”, the maintainers advise. The Apache Logging Services project released Apache Log4j 2.16.0 on Monday (December 13) after the first update, version 2.15.0, was found to be “incomplete in some non-default configurations and could allow an attacker to execute a denial-of-service (DoS) attack”, according to an Apache Software Foundation (ASF) blog post published yesterday (December 14). Users still on Java 7 should upgrade to the Log4j 2.12.2 release, said the ASF. The first flaw (CVE-2021-44228), which affects Log4j2 versions up to and including 2.14.1, allows an “attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled”. The project maintainers rushed out the first fix, which restricted JNDI LDAP lookups to localhost by default, after the proof of concept (PoC) surfacing on Twitter and GitHub. However, this patch then spawned a fresh flaw (CVE-2021-45046) that, if abused in certain contexts, could enable attackers to mount a DoS attack by crafting malicious input data using a JNDI Lookup pattern. Previous configuration-related mitigations do not mitigate the latest vulnerability, the ASF has emphasized. Apache also recommend that, while the Log4j 1.x series is not known to be affected by either CVE, users running versions from the first release line should still update to the latest release line, since the first has reached end of life and no longer receives security patches.

Apache has released Log4j version 2.17 to fix yet another high-severity denial-of-service vulnerability - tracked as CVE-2021-45105 with a CVSS score of 7.5 - that affects all versions from 2.0-beta9 to 2.16.0.The latest version introduced by the nonprofit Apache Software Foundation addresses a denial-of-service flaw introduced in 2.16 and all other versions.Previously, Apache had released Log4j version 2.16 to fix another issue designated as CVE-2021-45046 that could result in a remote code execution flaw, which stemmed from an "incomplete" fix for CVE-2021-44228, otherwise called the Log4Shell vulnerability.The latest patch comes after the U.S. Cybersecurity and Infrastructure Security Agency issued an emergency directive on Friday regarding the explosive Apache Log4j vulnerabilities. The directive requires federal civilian departments and agencies to immediately patch their systems or implement appropriate mitigation measures.

ATTACK TYPE

Zero-Day Vulnerability

CAUSE OF ISSUE

Lack of Patch Management

TYPE OF LOSS

System Compromise,
Reputation loss

SECURITY RESEARCHER EARNS PLAUDITS AFTER DISCOVERING YANDEX SSRF FLAW

Russian search and internet services giant Yandex has resolved a potentially serious server-side request forgery (SSRF) vulnerability discovered by Egyptian security researcher Momen Ali. His search to identify potential targets within Yandex's infrastructure using a variety of Google dorks, and the SSRF vulnerability he eventually uncovered. The root cause of the vulnerability was a misconfigured server forwarding requests to the hostname specified in the Proxy-Host HTTP header. "SSRF happened because of injecting HTTP headers such as X-Forwarded-Host, so in my case the SSRF was in HTTP header,". Ali used a combination of Burp Intruder, Burp Collaborator, and the Nuclei template scanner to uncover and validate the vulnerability.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Server Side Request Forgery	Server Misconfiguration	System Compromise

TEEN HACKER SCOOPS $4,500 BUG BOUNTY FOR FACEBOOK FLAW THAT ALLOWED ATTACKERS TO UNMASK PAGE ADMINS

"A 19-year-old hacker from Nepal has received a $4,500 bug bounty following their discovery of an easy-to-exploit vulnerability that allowed users to reveal the identity of page administrators. After digging around in the Facebook-for-Android app, ethical hacker Sudip Shah discovered an insecure direct object reference (IDOR) vulnerability that could have allowed an attacker to disclose the identity of a page administrator. The researcher added: "This could be escalated further to fetch the admin information of a huge number of pages by creating a script… and capturing the admin information from the broadcaster_id in the response to a new text file." The researcher added: "This could be escalated further to fetch the admin information of a huge number of pages by creating a script… and capturing the admin information from the broadcaster_id in the response to a new text file."

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Insecure Direct Object Reference	Broken Access Control Policy	Loss of PII Data

SAP SQUASHES SQL INJECTION, XSS BUGS IN DECEMBER PATCH ROUND

On Tuesday (December 14), the tech giant published a security advisory detailing the latest batch of patches, which includes fixes for vulnerabilities that can be exploited for code execution, denial of service (DoS), and to perform cross-site scripting (XSS) attacks. An SAP advisory lists code execution issues in the localized, Chinese version of SAP Commerce v. 2001. In total, 11 related CVEs point to flaws within XStream, a Java library used to serialize objects to XML. Before version 1.4.16, the library contained vulnerabilities allowing attackers to manipulate streams to expose data, to overload CPU resources, to perform server-side forgery requests (SSRF), and to load and execute arbitrary code, among other issues. The code execution issue, overall, has been assigned a near-maximum CVSS severity score of 9.9. SAP also resolved CVE-2021-44231 – CVSS score 9.9 – which is a code injection flaw caused by an error in text extraction features of the Translation Tools section in SAP ABAP Server & ABAP. If exploited, this vulnerability allows attackers to hijack the application.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Server Side Request Forgery	Lack of Patch Management	Application Compromise

SEVERE CHROME BUG ALLOWED RCE ON DEVICES RUNNING REMOTE HEADLESS INTERFACE

A fixed bug in Chrome allowed attackers to read and write local files and install malicious scripts on devices running the browser's headless interface, researchers at Contrast Security have discovered. Since 2017, Chrome has included a headless mode that allows developers to run an instance of the browser without launching the user interface. The headless browser can be controlled programmatically and debugged remotely and is intended for testing web applications and webpage functionality without human interaction. Contrast Security's Matt Austin showed that by using a malicious HTML file stored locally on the device running the headless browser, an attacker can read the contents of sensitive files and write arbitrary files to the device's hard drive.

ATTACK TYPE

Malware Attack

CAUSE OF ISSUE

Lack of Patch Management

TYPE OF LOSS

Loss of PII Data

ZERO-DAY VULNERABILITY IN HILLROM CARDIOLOGY DEVICES COULD ALLOW ATTACKERS FULL CONTROL

A high-severity vulnerability in several cardiac healthcare devices could allow attackers to access privileged accounts without a password and seize control of the devices. The authentication bypass flaw in certain products made by Hillrom exists when the devices have been configured to use single sign-on (SSO). It allows the manual entry of all active directory (AD) accounts provisioned within the application, meaning access will be granted without having to provide the associated password.

ATTACK TYPE

Privilege Escalation

CAUSE OF ISSUE

Lack of Authentication

TYPE OF LOSS

Active Directory Compromise

DRIVE-BY RCE IN WINDOWS 10 'CAN BE EXECUTED WITH A SINGLE CLICK'

A drive-by remote code execution (RCE) vulnerability in Windows 10 that can be triggered simply by clicking a malicious URL could allow attackers full access to a victim's files and data. The security flaw, an argument injection in the Windows 10/11 default handler for ms-officecmd: URIs, is present in Windows 10 via Internet Explorer 11/Edge Legacy browsers and Microsoft Teams. Microsoft has since released a patch, but researchers claim that the fix – applied five months after the bug report – "fails to properly address the underlying argument injection which is currently also still present on Windows 11".

ATTACK TYPE

Remote Code Execution

CAUSE OF ISSUE

Lack of Patch Management

TYPE OF LOSS

Data Loss

CRITICAL WEB SECURITY FLAWS IN KASEYA UNITRENDS BACKUP APPLIANCES REMEDIATED AFTER RESEARCHERS' DISCLOSURE

Developers have resolved a series of vulnerabilities in storage technologies from Kaseya, including two critical flaws that each posed a remote code execution risk. Two unauthenticated SQL injection vulnerabilities in the Kaseya Unitrends Backup Appliance (tracked as CVE-2021-43035) made it possible for potential attackers to inject arbitrary SQL queries under the Postgres superuser account. Each of the flaws (rated with a CVSS score of 9.8, close to the maximum severity of 10.0) posed a remote code execution risk to Kaseya Unitrends Backup Appliance running vulnerable versions of the software, ranging from 10.0.x-10.5.4.

ATTACK TYPE

Remote Code Execution

CAUSE OF ISSUE

Lack of Security Controls

TYPE OF LOSS

Data Loss

CRITICAL VULNERABILITIES IN OPEN SOURCE FORUM SOFTWARE NODEBB COULD LEAD TO RCE

Critical vulnerabilities in open source forum platform NodeBB could allow attackers to steal private information and access admin accounts, researchers have warned. The three software issues identified in a blog post are a path traversal bug, a cross-site scripting (XSS) flaw, and an authentication bypass vulnerability The path traversal bug (CVE-2021-43788) allowed users to access JSON files outside of the expected languages/ directory and could allow attackers to leak potentially sensitive files, for example the NodeBB config or exported user profiles with personally identifiable information. The XSS vulnerability (CVE-2021-43787) can be used by attackers to take over user accounts, including admin accounts. To be hijacked, victims only have to visit the profile or a forum post of a malicious user. Finally, the authentication bypass bug (CVE-2021-43786) allows attackers to directly execute commands on the server using just a single request.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Authentication Bypass	Lack of Authentication	Data Loss, Loss of PII Data

WORDPRESS SECURITY PLUGIN HIDE MY WP ADDRESSES SQL INJECTION, DEACTIVATION FLAWS

Hide My WP, a popular WordPress security plugin, contained a serious SQL injection (SQLi) vulnerability and a security flaw that enabled unauthenticated attackers to deactivate the software. Now patched, the bugs were discovered during an audit of several plugins on a customer's website by Dave Jong, CTO of Patchstack, which protects WordPress websites from vulnerabilities and runs a WordPress-focused bug hunting platform. The SQLi "is pretty severe", Jong told The Daily Swig. "It allows anyone to extract information from the database, it has no prerequisites. A tool such as SQLmap could easily exploit this vulnerability." The other vulnerability is less severe, "but could, under the right conditions, cause a malicious user to continue exploitation of a different vulnerability", added Jong. Both flaws are "very easy to exploit as they require no prerequisites", he warned.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
SQL Injection	Lack of Security Controls	Data Loss, Loss of PII Data

GOAUTODIAL VULNERABILITIES PUT CALL CENTER NETWORK SECURITY ON THE LINE

GOautodial, an open source call center software suite with 50,000 users around the world, has patched two vulnerabilities that could lead to information disclosure and remote code execution (RCE). Unearthed by Scott Tolley of the Synopsys Cybersecurity Research Center (CyRC), the first bug – tracked as CVE-2021-43175 – has been rated medium severity. The vulnerable versions of GOautodial validate the username and password incorrectly, allowing the caller to specify any values for these parameters and successfully authenticate. This allows the caller to name and call a second PHP file without having any valid credentials for the GOautodial system. The first vulnerability – broken authentication on the GOautodial API – allows any attacker with network access to the GOautodial server to simply request a set of configuration data from it, without any kind of valid user account or password. This configuration data includes sensitive data such as default passwords for other devices and applications on the network that an attacker could then leverage to attack other components of the system. Another vulnerability, CVE-2021-43176, allows any authenticated user at any level to perform remote code execution, allowing them to gain complete control over the GOautodial application on the server. Rated high severity, it allows an attacker to steal the data from fellow employees and customers, and even rewrite the application to introduce malicious behavior.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Remote Code Execution	Lack of Authentication	Application Compromise

MICROSOFT WARNS OF EASY WINDOWS DOMAIN TAKEOVER VIA ACTIVE DIRECTORY BUGS

Microsoft warned customers today to patch two Active Directory domain service privilege escalation security flaws that, when combined, allow attackers to easily takeover Windows domains. The company released security updates to address the two security vulnerabilities (tracked as CVE-2021-42287 and CVE-2021-42278 and reported by Andrew Bartlett of Catalyst IT) during the November 2021 Patch Tuesday. Redmond's warning to immediately patch the two bugs — both allowing attackers to impersonate domain controllers — comes after a proof-of-concept (PoC) tool that can leverage these vulnerabilities was shared on Twitter and GitHub on December 11. When combining these two vulnerabilities, an attacker can create a straightforward path to a Domain Admin user in an Active Directory environment that hasn't applied these new updates. This escalation attack allows attackers to easily elevate their privilege to that of a Domain Admin once they compromise a regular user in the domain.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Privilege Escalation	Lack of Patch Management	System Takeover

FBI: STATE HACKERS EXPLOITING NEW ZOHO ZERO-DAY SINCE OCTOBER

"The Federal Bureau of Investigation (FBI) says a zero-day vulnerability in Zoho's ManageEngine Desktop Central has been under active exploitation by state-backed hacking groups (also known as APTs or advanced persistent threats) since at least October. Since at least late October 2021, APT actors have been actively exploiting a zero-day, now identified as CVE-2021-44515, on ManageEngine Desktop Central servers. The APT actors were observed compromising Desktop Central servers, dropping a webshell that overrides a legitimate function of Desktop Central, downloading post-exploitation tools, enumerating domain users and groups, conducting network reconnaissance, attempting lateral movement and dumping credentials. The security flaw, patched by Zoho in early December, is a critical authentication bypass vulnerability attackers could exploit to execute arbitrary code on vulnerable Desktop Central servers. CISA added CVE-2021-44515 to its Known Exploited Vulnerabilities Catalog on December 10, requiring federal agencies to patch it before Christmas under Binding Operational Directive (BOD) 22-01.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Zero-Day Vulnerability	Lack Of Security Patches	System Takeover

T-MOBILE SAYS IT BLOCKED 21 BILLION SCAM CALLS THIS YEAR

T-Mobile says it blocked 21 billion scam, spam, and unwanted robocalls this year through its free Scam Shield robocall and scam protection service, amounting to an average of 1.8 billion scam calls identified or blocked every month. Furthermore, based on data through early December 2021, the carrier fund that scam call traffic has reached an all-time high, jumping over 116% from 2020 to a total of roughly 425 million scam call attempts every week. Last year, when it announced the Scam Shield service, T-Mobile said it could detect or block approximately 12 billion scam calls in 2019 and that around 30 million Americans fell victim to a phone scam within 12 months. The scammers' favorite targets throughout 2021 were people from Texas, Florida, Arizona, and Georgia, the most targeted being those in the Dallas/Fort Worth area code.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS
Vishing	Lack of Security Awareness	Unknown

CREDIT CARD INFO OF 1.8 MILLION PEOPLE STOLEN FROM SPORTS GEAR SITES

Four affiliated online sports gear sites have disclosed a cyberattack where threat actors stole credit cards for 1,813,224 customers. While not much is known about the attack, a law firm representing the four websites stated that personal information and credit card information, including full CVV, were stolen on October 1st, 2021. The affected websites are the following: Tackle Warehouse LLC (tacklewarehouse.com), Running Warehouse LLC (runningwarehouse.com), Tennis Warehouse LCC (tennis-warehouse.com), Skate Warehouse LLC (skatewarehouse.com). The sites first learned of the breach on October 15th, and after an investigation, confirmed on November 29th the customers that had their payment information stolen. The details that have been compromised as a result of this incident are the following: Full name, Financial account number, Credit card number (with CVV), Debit card number (with CVV), Website account password. After the conclusion of the investigation, the websites sent notices to the affected individuals on December 16th, 2021.

ATTACK TYPE

Data Breach

CAUSE OF ISSUE

Lack of Data Protection Policies and Methodologies

TYPE OF LOSS

Loss of PII Data

CISA URGES VMWARE ADMINS TO PATCH CRITICAL FLAW IN WORKSPACE ONE UEM

CISA has asked VMware admins and users today to patch a critical security vulnerability found in the Workspace ONE UEM console that threat actors could abuse to gain access to sensitive information. Workspace ONE Unified Endpoint Management (ONE UEM) is a VMware solution for over-the-air remote management of desktops, mobile, rugged, wearables, and IoT devices. The flaw tracked as CVE-2021-22054 is a server side request forgery (SSRF) vulnerability with a severity rating of 9.1/10 and impacting multiple ONE UEM console versions. Unauthenticated threat actors can exploit this vulnerability remotely in low-complexity attacks without user interaction.

ATTACK TYPE

Server Side Request Forgery

CAUSE OF ISSUE

Lack Of Security Patches

TYPE OF LOSS

Data Loss

MULTIPLE VULNERABILITIES IN MICROSOFT TEAMS COULD SPOOF URLS, LEAK IP ADDRESSES

"Security vulnerabilities in Microsoft Teams could allow an attacker to spoof link previews, leak IP addresses, and even access internal services. A total of four vulnerabilities in the video conferencing app were discovered by a team of security researchers from Positive Security, who revealed the findings in a blog post released. The four findings are a server-side request forgery (SSRF) vulnerability and a URL preview spoofing bug in the web and desktop application, and for Android users, an IP address leak vulnerability and a denial-of-service (DoS) vulnerability. In the Microsoft Teams URL preview feature, the URL is not filtered, which could lead to a limited SSRF that could leak information such as the response time, code, size, and open graph data, researchers explained. This could be used for internal port scanning and sending HTTP-based exploits to the discovered web services.The researchers mentioned that: "An attacker could use the SSRF to scan for internal HTTP(s) services and send requests with the Log4Shell payload in the request URI to all of them to try to exploit vulnerable services that are not reachable from the internet."

ATTACK TYPE

Server Side Request Forgery, DOS

CAUSE OF ISSUE

Lack of Secure data validation

TYPE OF LOSS

System Compromise and Data Loss

SAFE BROWSING: GOOGLE FIXES CHROME SITE ISOLATION BYPASS BUG

A set of features meant to speed up web page loading in Chrome contained a bug that allowed attackers to bypass the browser's Site Isolation feature, a security researcher has discovered. Chrome uses Same Origin Policy to prevent websites from accessing each other's data inside the browser, but sometimes, subtle security bugs such as Spectre open pathways to bypassing these policies.The exploit starts when a malicious website uses 'navigation preload', a feature that loads a URL in parallel to booting the service worker. In this case, the malicious code uses a URL loader with Cross-Origin Read Blocking (CORB) disabled. CORB is an algorithm that prevents cross-origin resource loads in web browsers before they reach the web page.Once the CORB-disabled URL loader is ready, it is passed on to the service worker, where it loads the requested content and destroy itself. The URL loader is supposed to prevent redirects, but since the service worker has access to URL loader interface, it can modify its behavior to follow the redirect and read the full response even if it's from a cross-origin domain.Moreover, the Site Isolation feature will not block the code from accessing the off-bounds data.In proof-of-concept code, the researcher shows how an attacker can use the bug to request a Gmail URL and get access to a user's cookies and data.

ATTACK TYPE

Zero Day Vulnerability

CAUSE OF ISSUE

Lack of Patch Management

TYPE OF LOSS

Data Loss

UBISOFT CONFIRMS JUST DANCE VIDEO GAME DATA BREACH

Ubisoft has announced a data breach after unknown actors targeted its popular video game franchise, Just Dance.The games developer confirmed that customer information may have been accessed after attackers took advantage of a “misconfiguration” to steal data.A statement from Ubisoft said that the breach was limited to ‘technical identifiers’ including GamerTags, profile IDs, and device IDs, as well as recordings of Just Dance videos that were uploaded to be shared publicly with the in-game community and/or on social media profiles.It adds: “This incident was the result of a misconfiguration, that once identified, was quickly fixed, but made it possible for unauthorized individuals to access and possibly copy some personal player data.“Our investigation has not shown that any Ubisoft account information has been compromised as a result of this incident.”Ubisoft has advised all Just Dance users to reset their passwords and to use two-factor authentication.

ATTACK TYPE

Data Breach

CAUSE OF ISSUE

Security Misconfiguration

TYPE OF LOSS

Data Loss

CLOP RANSOMWARE ACTORS LEAK UK POLICE DATA

Personal information and records of 13 million people held by some of Britain's police forces has been stolen by Russian hackers, according to a news report.U.K. newspaper The Daily Mail Online reported that the cybercriminal gang Clop has released some of the data on the dark web after successfully breaching Scotland-based managed service provider Dacoll, which handles access to the Police National Computer.The gang is reported to have threatened to release more data, and the report also says Clop demanded a ransom from the company after launching a phishing attack in October that gave it access to the personal information and records of 13 million people.

ATTACK TYPE

Phishing

CAUSE OF ISSUE

Lack of Security Awareness

TYPE OF LOSS

Data Loss

ACTIVE DIRECTORY BUGS ENABLE WINDOWS DOMAIN TAKEOVER

Microsoft is urging customers to apply patches issued in November for two Active Directory domain controller bugs, following publication of a proof-of-concept tool that leverages these bugs, which when chained can allow easy Windows domain takeover.The vulnerabilities tracked as CVE-2021-42287 and CVE-2021-42278 allow threat actors to take over Windows domains. The flaws were fixed during the November 2021 Patch Tuesday, but a few weeks later, on Dec. 12, a proof-of-concept exploit leveraging these vulnerabilities was publicly disclosed. These two vulnerabilities allow attackers to take over Windows domains, and they would have had great repercussions had they emerged at another time. However, they were overshadowed by the Log4j attacks and could only find a place on the agenda when Microsoft issued an alert on Dec. 2. Both vulnerabilities are Windows Active Directory domain service privilege escalation vulnerabilities and are rated as critical, with a CVSS score of 7.5 out of 10, according to Microsoft.

ATTACK TYPE

Privilege Escalation

CAUSE OF ISSUE

Lack of Data Protection Policies and Methodologies

TYPE OF LOSS

System Takeover

500,000 ANDROID USERS VICTIMIZED BY MALWARE-INFECTED APP

A Trojanized malicious software known as "Joker" malware has made a comeback and was detected in a Google Play app downloaded more than 500,000 times, researchers say.The Joker malware has reportedly existed since at least 2017, and attackers have used it widely.Global mobile security company Pradeo discovered that the malicious software had made a comeback via Google Play and says threat actors continue to use it to victimize users worldwide. The researchers for Pradeo say that the malware has propagated across Android and third-party app stores.More than 500,000 users downloaded the app - called Color Message - that was found to contain the malware. Researchers also say stolen data siphoned through the malicious app appears to link back to servers in Russia, according to the research by Pradeo.Ars Technica says it contacted Google to bring attention to the malware in Color Message. Google immediately took the app down from Google Play but did not offer additional comments, the company says.

ATTACK TYPE

Malware Attack

CAUSE OF ISSUE

Lack of Malware Protection tools

TYPE OF LOSS

Data Loss

IRANIAN THREAT ACTOR USES SLACK API TO TARGET ASIAN AIRLINE

An Iranian state-sponsored threat group is using free workspaces on messaging platform Slack to deploy a backdoor in an Asian airline's system, according to researchers.The backdoor, dubbed Aclip, may have enabled the threat actor to access the airline's passenger reservations data, an IBM Security X-Force report says.he backdoor, it says, sends system information, files and screenshots of the data on the victim systems to its command-and-control server, corresponding to the commands received.-The threat actor's focus was surveillance, as only files with "reservation management" in their names were found on the threat actor's C2 server, the report says. It does not disclose the contents of the exfiltrated archive files.

ATTACK TYPE

Malware Attack

CAUSE OF ISSUE

Lack of Malware Protection tools

TYPE OF LOSS

Data Loss

GHANA GOVT AGENCY EXPOSED 700K CITIZENS' DATA IN A DATABASE MESS UP

VPNMentor's cybersecurity researchers Noam Rotem and Ran Locar reported that Ghana's National Service Secretariate – NSS – suffered a massive database misconfiguration that exposed data of up to 700,000 citizens from across the country, amounting to 55GB of data.Researchers believe this breach poses a great risk for the Ghanian government officials associated with the agency and thousands of its citizens. The exposed database was discovered on 29 September 2021, and NSS and CERT-GH were notified between 6th and 12th October 2021. According to VPNMentor's report, the NSS was using Amazon Web Services (AWS), where it stored over 3 million files from its different programs. Some of the files in the cloud storage account were password-protected, most of the files were still exposed to public access as well as the database.

ATTACK TYPE

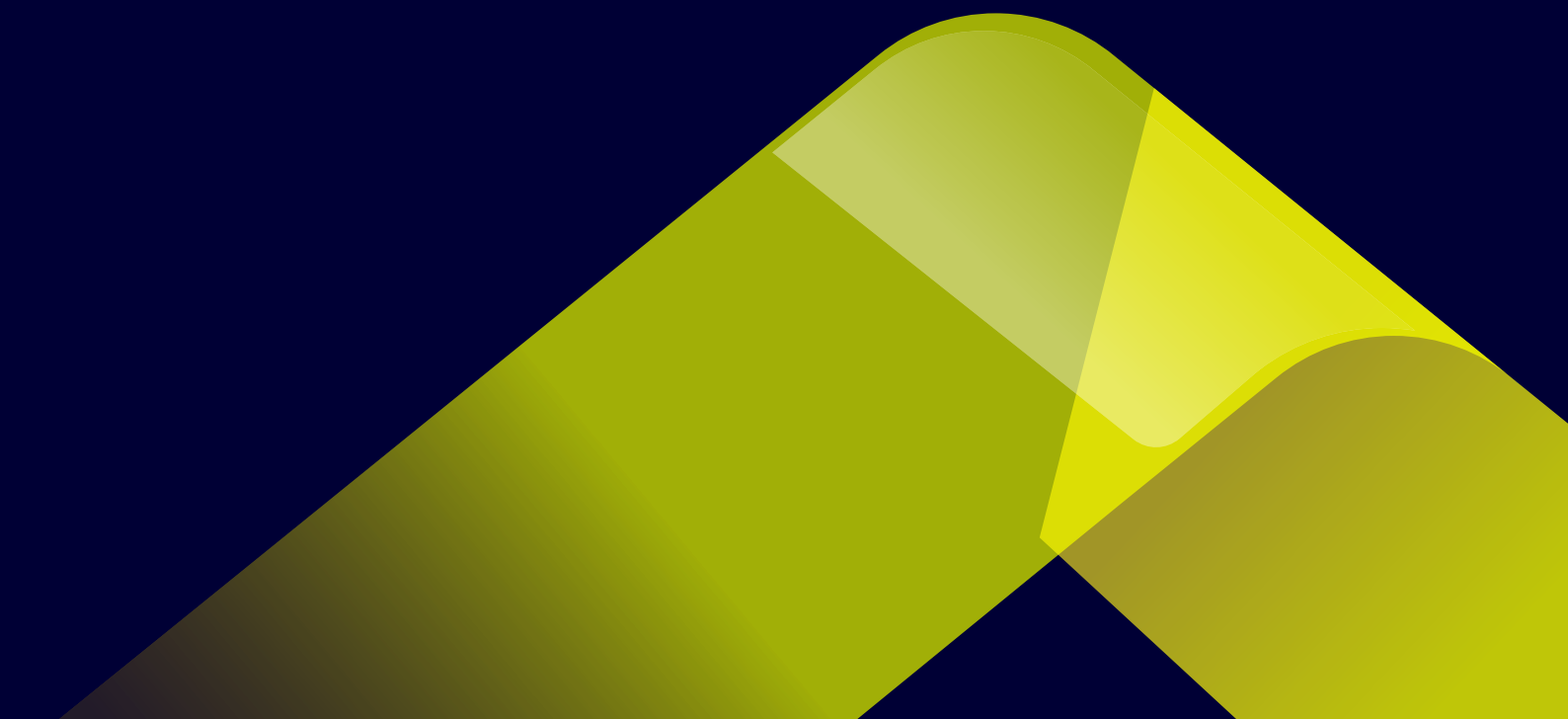
Data Breach

CAUSE OF ISSUE

Database Misconfiguration

TYPE OF LOSS

Data Loss



CONCLUSION

According to an article, online threats has risen by as much as six times their usual levels recently as the Covid 19 pandemic provided greater scope for cyber attacks. All the attacks mentioned above - their types, the financial and reputation impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like a drop in an ocean. There are more unreported than that meets the eye. Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being 'lack of awareness. Well, as the saying goes,

"PREVENTION IS BETTER THAN CURE" - BE IT COVID-19 OR CYBER THREATS.

Briskinfosec is ready to help you in your journey to protect your information infrastructure and assets. We assure you that we will help you to keep your data safe and also give you clear information on your company's current status and what are the steps needed to be taken to stay away from any kind of cyber attack.

CORPORATE OFFICES

INDIA

Briskinfosec
No:21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034.
+91 86086 34123 | 044 4352 4537

USA

3839 McKinney Ave,
Ste 155 - 4920,
Dalls TX 75204.
+1 (214) 571 - 6261

UK

Imperial House 2A,
Heigham Road, Eastham,
London E6 2JG.
+44 (745) 388 4040

BAHRAIN

Urbansoft, Manama Center, Entrance One,
Building No.58, No.316, Government Road,
Manama Area, Kingdom of Bahrain.
+973 777 87226

contact@briskinfose.com | www.briskinfosec.com