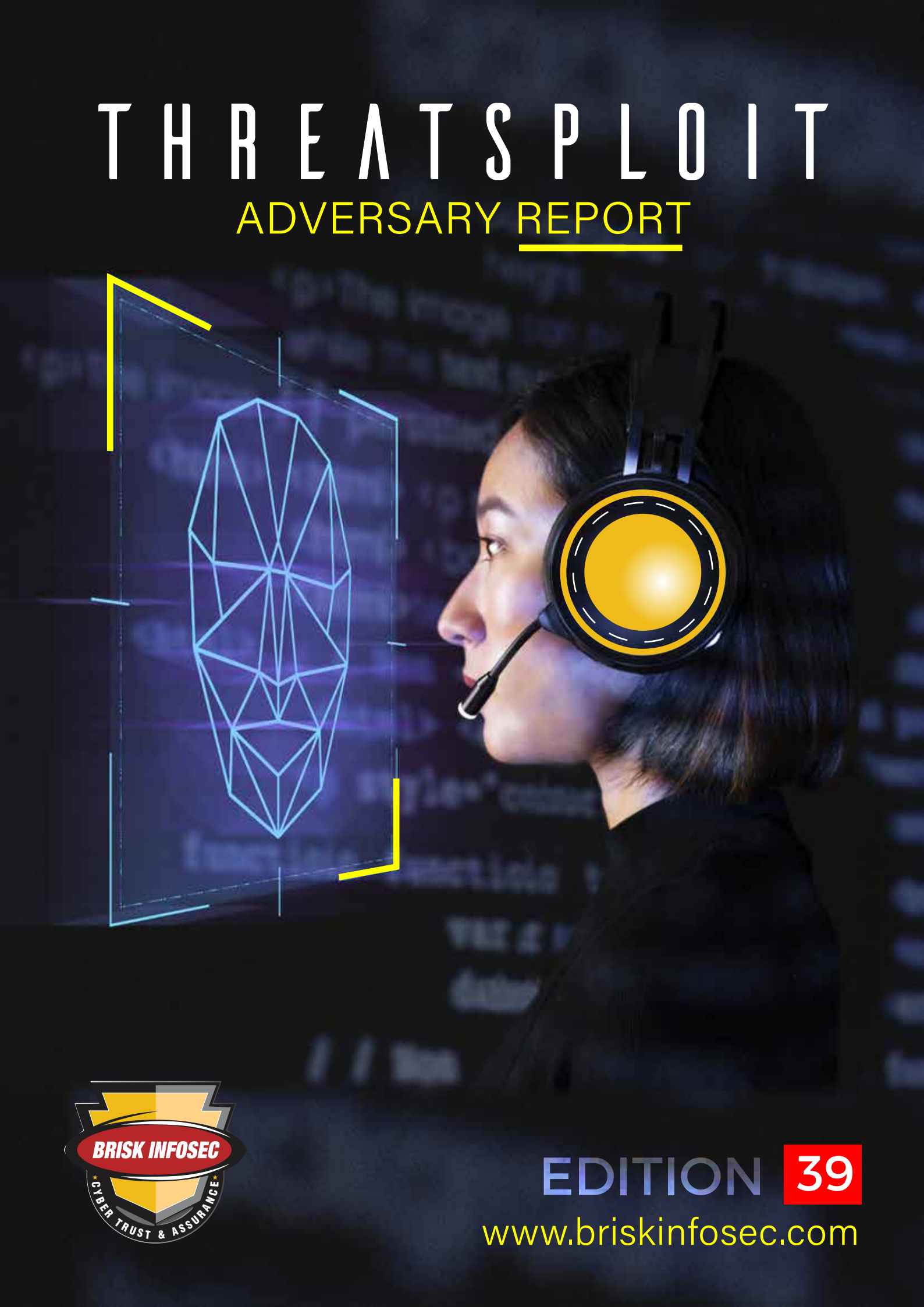
THREATSPLOIT

ADVERSARY REPORT



BRISK INFOSEC

CYBER TRUST & ASSURANCE

EDITION 39

www.briskinfosec.com

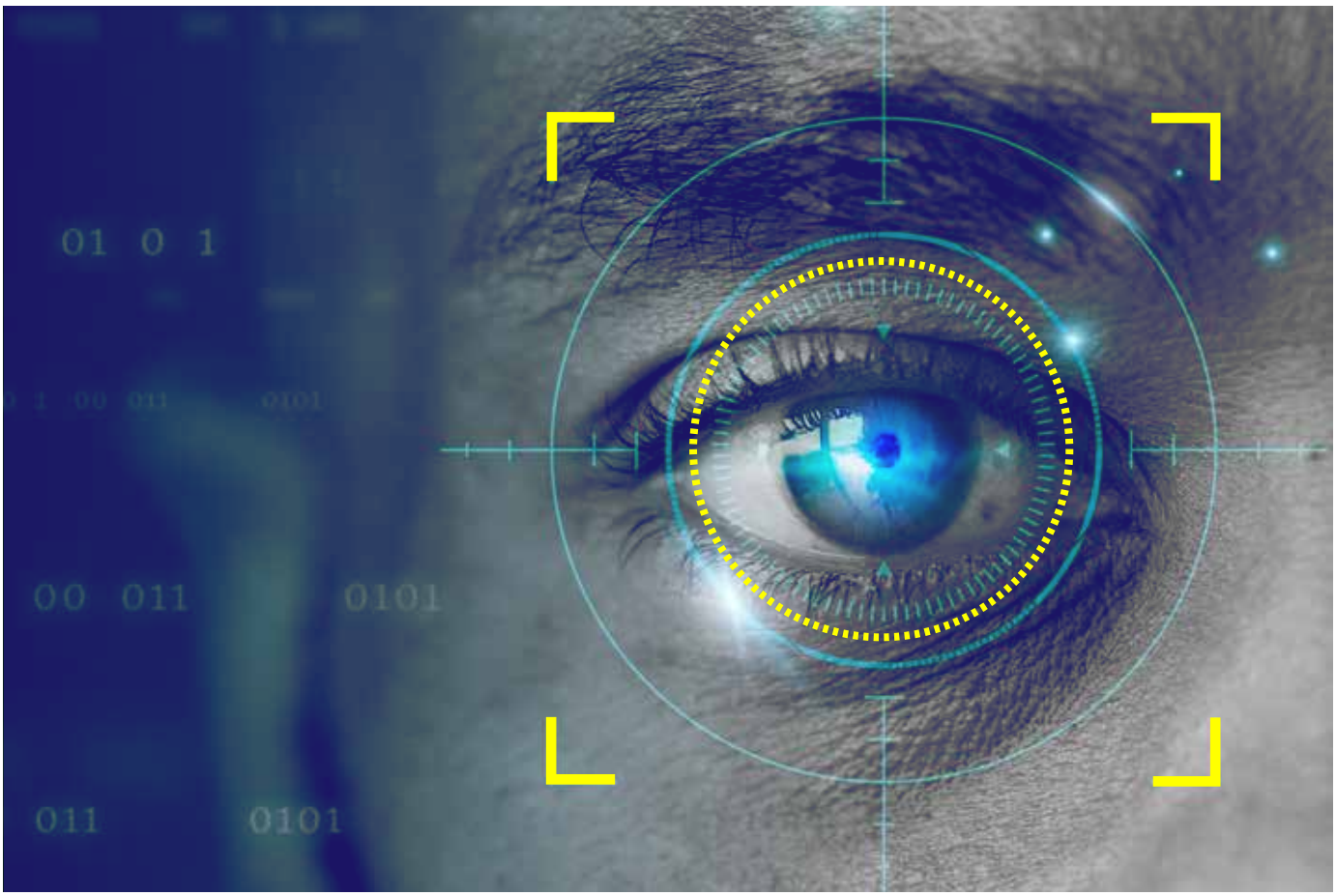
INTRODUCTION

Welcome to the Threatsploit Report of November 2021 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 -TAR

ACCENTURE

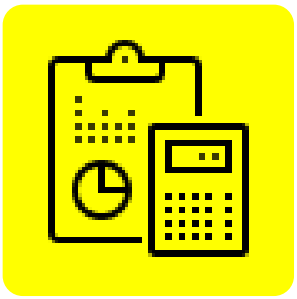
ATTACK TYPE
Data Breach-Sensitive Data Exposure

Ransomware Attack Breached Proprietary Data

The consultancy Accenture has confirmed that "irregular activity" in its IT networks last quarter, which it disclosed in August, also resulted in a breach of sensitive information. Dublin-based Accenture disclosed the data breach on Friday in its annual report for its fiscal year ending Aug. 31, which it filed as a form 10-K to the U.S. Securities and Exchange Commission, as Bleeping Computer first reported.

The LockBit 2.0 ransomware-as-a-service operation claimed credit for the attack, listing Accenture on its data-leak site as a victim and threatening to leak stolen data unless the consultancy paid a ransom. On its leak site, LockBit now lists for download 2,384 directories - which security experts say included even more subdirectories - as having been stolen from Accenture. By Aug. 22, the group had finished leaking the stolen data for free download from its data-leak site.

CAUSE OF ISSUE
Lack of Data Protection Policies & Methodologies



TYPE OF LOSS
Sensitive Company Data

Twitch breach leads to leak of source code and streamer earnings data

A breach at Twitch, the Amazon-owned service that specializes in video game live streaming, has exposed the apparent earnings of e-sports stars and other sensitive information. The hack and subsequent leak of data has revealed source code, internal tools, and hashed user passwords. The leak also reportedly spilled data on a prototype competitor to the Steam platform, codenamed Vapor, from Amazon Game Studios. Anonymous attackers leaked a 125 GB torrent featuring Twtich source which they publicised through 4chan. The leak was designed to “foster more disruption and competition in the online video streaming space”, the attacker claimed. In a statement on its official blog, Twitch confirmed the hack on its systems while attempting to downplay users’ potential concerns about the impact of the breach.

ATTACK TYPE
Data Breach – Souce Code Leakage

CAUSE OF ISSUE
Lack of Data Protection Policies & Methodologies

US clothing brand Next Level Apparel reports phishing-related data breach

Next Level Apparel, a US clothing manufacturer and e-commerce operator, has alerted customers to a data breach connected to the compromise of employee mailboxes. "A limited number of employees' email accounts" were compromised via phishing, which gave cybercriminals "access to the contents of the accounts at various times between February 17, 2021 and April 28, 2021," said Next Level Apparel in a press release issued on October 5. This "resulted in unauthorized access to information contained in some email accounts, including names accompanied by Social Security numbers, financial/checking account numbers, payment card numbers, driver's license numbers, and limited medical/health information".

ATTACK TYPE

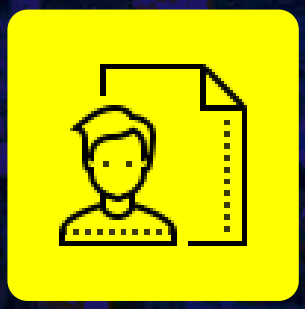
Phishing Attack - Unauthorized Access to Mail Accounts

CAUSE OF ISSUE

Lack of Security Awareness for Personnel

TYPE OF LOSS

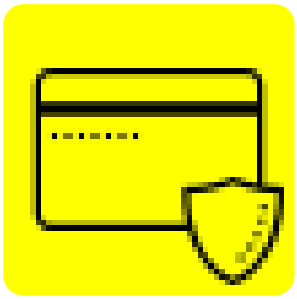
Unauthorized Access to User Accounts



US retailer Neiman Marcus notifies 4.6 million customers of data breach

US retail giant Neiman Marcus Group is alerting 4.6 million customers to a data breach that involves payment card and virtual gift card information. The company, which runs 37 luxury department stores in 17 states, said an unauthorized party obtained information associated with customers' online accounts in May 2020. It said it discovered in the incident in September, some 17 months later.

Stolen data "may have included names and contact information; payment card numbers and expiration dates (without CVV numbers); Neiman Marcus virtual gift card numbers (without PINs); and usernames, passwords, and security questions and answers associated with Neiman Marcus online accounts", said the company in a press release issued on September 30. Neiman Marcus said 3.1 million payment and virtual gift cards were impacted, but more than 85% of these were "expired or invalid".



ATTACK TYPE

Data Breach - Sensitive Data Exposure

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

TYPE OF LOSS

Loss of Payment Card & Customer Information

RCE vulnerabilities in open source software Cachet could put users at risk

Multiple security vulnerabilities in open source status page system Cachet could allow an attacker to execute arbitrary code and steal sensitive data, researchers have warned. Cachet is a project that allows users to do such tasks as listing service components, reporting incidents, and customizing the look of their status page, among other features. However three vulnerabilities in the software, discovered by researchers from SonarSource, could put its users at risk of remote takeover. The first bug (CVE-2021-39172) is a newline injection that is triggered when users update an instance's configuration, such as the email settings. A second vulnerability (CVE-2021-39174) is also related to this feature, and allows attackers to exfiltrate secrets that are stored in the configuration file – for example, database passwords and framework keys. The last bug (CVE-2021-39173) is "much simpler" according to researchers, and allows an attacker to change the setup process even if the target instance is already fully configured.

ATTACK TYPE

Data Breach - Sensitive Data Exposure

CAUSE OF ISSUE

Lack of Secure Patch Management Solution

TYPE OF LOSS

System Compromise, Loss of Sensitive Data

Multiple XSS vulnerabilities in child monitoring app Canopy 'could risk location leak'

A security researcher has reported multiple cross-site scripting (XSS) vulnerabilities in a child monitoring app that could leak data including a minor's location. Tripwire's Craig Young said that he discovered the security flaws in Canopy after the application was advertised to him by his child's school. Canopy allows parents to control how much screen time their children have on a device, manage the device itself and all communications, and prevent the child from accessing inappropriate content. The researcher found that a child's request explanation can contain XSS which executes in dashboard, a parent's rejection explanation can contain XSS which executes on a kid's phone, and a URL referenced in a request can contain XSS which is executed in the dashboard. An attacker with knowledge of these flaws could inject a new script into the dashboard for any or all Canopy parent accounts. This could give them access to a whole host of data belonging to the family, including the child's location.

ATTACK TYPE

Cross Site Scripting (XSS) Vulnerability

CAUSE OF ISSUE

Lack of Secure Input Validation

TYPE OF LOSS

Leakage of Location, Phishing Attacks

Injection Vulnerabilities in popular WordPress plugin could expose credentials, allow admin access

Vulnerabilities in a popular WordPress plugin Fastest Cache could allow an attacker to gain access to credentials and takeover an admin account. The security flaws in the extension, which has more than one million active downloads, were discovered during an internal audit of the software by Jetpack Security. The first flaw, an SQL injection vulnerability which has a CVSS score of 7.7, could grant attackers access to privileged information from an affected site's database, for example usernames and hashed passwords. This SQL injection bug can only be exploited if the classic-editor plugin is also installed and activated on the site.

Researchers also found a cross-site scripting (XSS) bug via a cross-site request forgery (CSRF) flaw that has a CVSS score of 9.6. Exploitation of this vulnerability would allow an attacker to perform the same actions as their victim, potentially an admin user, had privileges to enact.

ATTACK TYPE

Zero Day Vulnerability – Injection Vulnersbilities

CAUSE OF ISSUE

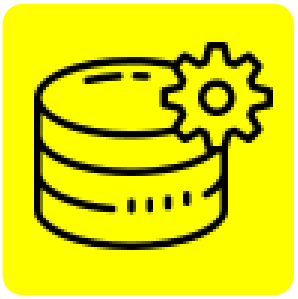
Lack of Patch Management

TYPE OF LOSS

Loss of User Account Data

Apache HTTP Server update fails to squash path traversal, RCE bugs

A patch that was released to fix a path traversal bug in Apache HTTP Server is insufficient in protecting against the vulnerability and could allow for remote code execution (RCE). As previously reported by The Daily Swig, the high-impact vulnerability was thought to have been fixed in Apache Server version 2.4.50. However not only did the update fail to resolve the issue, developers of the software are also now warning it presents a bigger security issue than previously thought. In a security advisory, the team behind Apache HTTP Server revealed that the update does not protect against a critical RCE bug, which is being exploited in the wild.



The blog post reads: "It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. "An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. "If files outside of these directories are not protected by the usual default configuration 'require all denied', these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution."

ATTACK TYPE

Zero Day Vulnerability – Apache 2.4.49 Path Traversal and RCE

CAUSE OF ISSUE

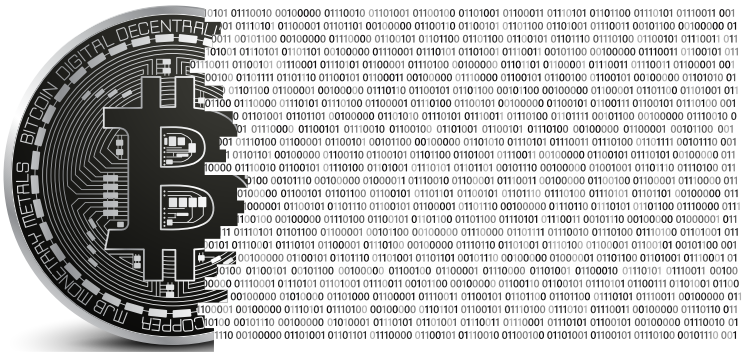
Lack of Patch Management Solutions

TYPE OF LOSS

Compromise of Server

Bitcoin.org hack nets give a way scammers $17,000 overnight

Cryptocurrency resource Bitcoin.org appears to be running normally again following a cyber-attack that commandeered the domain for a giveaway scam. The website was taken down in the early hours of yesterday morning (September 23) after a pop-up message began appearing that promised visitors they could double their money by sending cash to a bitcoin wallet. According to screenshots taken by CoinDesk, the message said the Bitcoin Foundation was "giving back to the community" with an offer that was open only to the first 10,000 participants. The message included a QR code and address for the fraudsters' wallet. Visitors were reportedly unable to navigate away from the pop-up. The scammers appear to have accrued more than $17,000 worth of Bitcoin from 10 transactions, and have already emptied the wallet, as documented by Blockchain.com.



ATTACK TYPE

Social Engineering & Scamming

CAUSE OF ISSUE

Lack of Security Awareness for Personnel

TYPE OF LOSS

Loss of User Data

ATTACK TYPE

Data Breach-Sensitive Data Exposure

Navistar confirms data breach involved employee healthcare information

An investigation at US truck maker Navistar has revealed that a data breach on its systems exposed employee healthcare information. Navistar hired external cybersecurity experts and began an investigation after learning of a security incident on May 20. By the end of May, the firm had confirmed that an "unauthorized third party had accessed and taken certain data from Navistar's IT systems". On June 7, Navistar filed 8-K papers with the US Security and Exchange Commission, warning investors about the incident. The notification generated press coverage about the incident from Reuters and other outlets, as investigators continued to access the scope and impact of the incident. By August 20, Navistar's team had confirmed that attackers had "accessed and taken" the personal information of participants to its healthcare and life insurance plans. The potentially compromised data included the full names, addresses, dates of birth, and Social Security numbers of an unspecified number of Navistar employees past and present, according to an updated statement by Navistar on the breach.

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

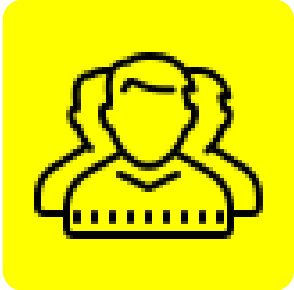
TYPE OF LOSS

Loss of Healthcare Data

Node.js was vulnerable to a novel HTTP request smuggling technique

The maintainers of Node.js have patched two HTTP request smuggling (HRS) vulnerabilities in the JavaScript runtime environment, including one found using what appears to be a new HRS technique. A server-side technology that allows JavaScript to be executed out of the browser, Node.js is an increasingly popular way of developing and hosting web apps. HTTP request smuggling interferes with how websites process sequences of HTTP requests received from users. The first, CVE-2021-22959, allows HTTP request smuggling due to spaces in headers, with the HTTP parser accepting requests with a space after the header name and before the colon. "This is a classic HRS technique," says Grenfeldt.

"Node interprets 'Content-Length : 5' as 'Content-Length: 5'. If combined with a proxy which ignores such headers, but forwards them unmodified, then HRS is possible. There have been many issues in the past similar to this. "Interestingly, Regilero has also reported this exact issue to Node earlier, together with a bunch of other issues; they were collectively assigned CVE-2016-2086. All of the issues were fixed, except for the space + colon issue." Meanwhile, CVE-2021-22960 appears to represent a novel HRS technique, whereby combining bad line termination in one of the proxies investigated and incorrect parsing of chunk extensions in Node allows request smuggling.



ATTACK TYPE

Zero Day Vulnerability - HTTP Request Smuggling

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Loss of User Data

Microsoft fixes Surface Pro 3 TPM bypass with public exploit code

The security flaw, dubbed TPM Carte Blanche by Google security researchers who discovered it, is tracked as CVE-2021-42299 and can be exploited in high complexity attacks by attackers with access to the owner's credentials or physical access to the device. Device Health Attestation is a cloud and on-premises service that validates TPM and PCR logs for endpoints and informs Mobile Device Management (MDM) solutions if Secure Boot, BitLocker, and Early Launch Anti-malware (ELAM) are enabled, Trusted Boot is correctly signed, and more. By exploiting CVE-2021-42299, attackers can poison the TPM and PCR logs to obtain false attestations, allowing them to compromise the Device Health Attestation validation process. "Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. Windows uses these PCR measurements to determine device health," Microsoft explains. "A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks." "The attacker can prepare a bootable Linux USB stick to minimize the interactions required with the target device (e.g., as an Evil Maid attack)," added Chris Fenner, the Google software engineer who found the bug.

Acer confirms breach of after - sales service systems in India

Taiwanese computer giant Acer has confirmed that its after-sales service systems in India were recently breached in what the company called "an isolated attack." "Upon detection, we immediately initiated our security protocols and conducted a full scan of our systems. We are notifying all potentially affected customers in India," an Acer Corporate Communications spokesperson told BleepingComputer.

"The incident has been reported to local law enforcement and the Indian Computer Emergency Response Team, and has no material impact to our operations and business continuity." While Acer didn't provide details regarding the attackers' identity behind this incident, a threat actor has already claimed the attack on a popular hacker forum, saying that they stole more than 60GB of files and databases from Acer's servers. The allegedly stolen data includes client, corporate, and financial data and login details belonging to Acer retailers and distributors from India.

ATTACK TYPE

Data Breach - Sensitive Data Theft

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

TYPE OF LOSS

Loss of Company Data & Reputation Loss

Emergency Apple iOS 15.0.2 update fixes zero-day used in attacks

Apple has released iOS 15.0.2 and iPadOS 15.0.2 to fix a zero-day vulnerability that is actively exploited in the wild in attacks targeting Phones and iPads. This vulnerability, tracked as CVE-2021-30883, is a critical memory corruption bug in the IOMobileFrameBuffer allowing an application to execute commands on vulnerable devices with kernel privileges. As kernel privileges allow the application to execute any command on the device, threat actors could potentially use it to steal data or install further malware. While Apple has not provided any details on how this vulnerability was used in attacks, they state that there are reports of it being actively used in attacks. "Apple is aware of a report that this issue may have been actively exploited," the company said in a security advisory published earlier today.

ATTACK TYPE

Zero Day Vulnerability - Memory Corruption RCE

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Loss of PII data, Loss of User Privacy

LibreOffice, OpenOffice bug allows hackers to spoof signed docs

LibreOffice and OpenOffice have pushed updates to address a vulnerability that makes it possible for an attacker to manipulate documents to appear as signed by a trusted source. Although the severity of the flaw is classified as moderate, the implications could be dire. The digital signatures used in document macros are meant to help the user verify that the document hasn't been altered and can be trusted. The discovery of the flaw, which is tracked as CVE-2021-41832 for OpenOffice, was the work of four researchers at the Ruhr University Bochum. The same flaw impacts LibreOffice, which is a fork of OpenOffice spawned from the main project over a decade ago, and for their project is tracked as CVE-2021-25635.

ATTACK TYPE

Zero Day Vulnerability - Manipulation of Digital Signature

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Loss of User Data

BrewDog exposed data for over 200,000 shareholders and customers

BrewDog, the Scottish brewery and pub chain famous for its crowd-ownership model and the tasty IPAs, has irreversibly exposed the details of 200,000 of its shareholders and customers. The exposure lasted for over 18 months and the point of the leak was the firm's mobile app, which gives the 'Equity Punks' community access to information, discounts at bars, and more. Apart from the fact that anyone could access the sensitive details of other app users, shareholders and customers of BrewDog, the implications of this finding also hit the company itself.

An abuser of the flaw could get endless free beer and discounts by generating QR codes from "loaded" accounts. The flaw existed since March 2020, when BrewDog started using hard-coded tokens with app version 2.5.5. Unfortunately BrewDog's team missed this flaw for an extended period of time and failed to secure their token system on the multiple subsequent releases that followed. Eventually, the issue was patched with version 2.5.13 which came out on September 27, 2021. BrewDog though chose not to disclose anything important in the changelog notice of that release.

ATTACK TYPE

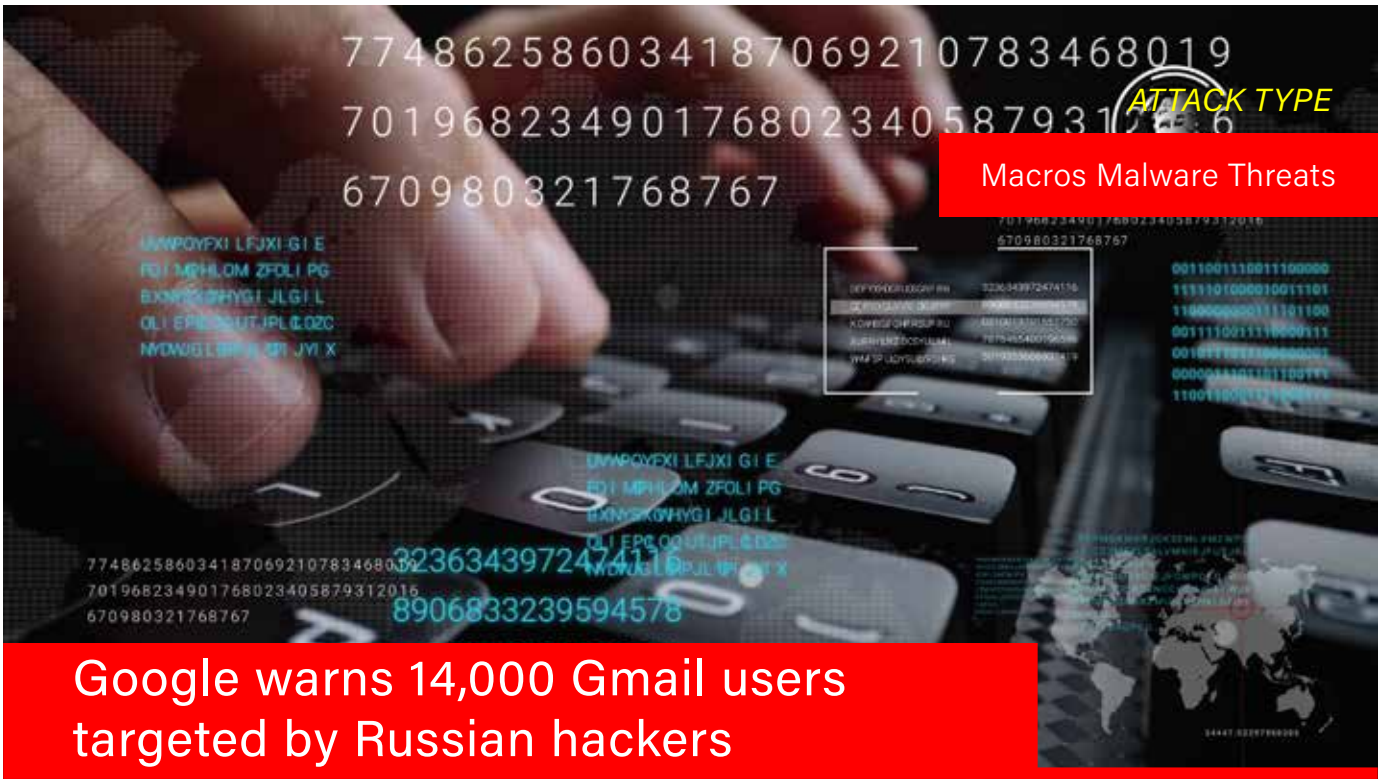
Data Breach - Sensitive Data Exposure

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

TYPE OF LOSS

Loss of Customer Data



Google warns 14,000 Gmail users targeted by Russian hackers

Microsoft will soon begin disabling Excel 4.0 XLM macros by default in Microsoft 365 tenants to protect customers from malicious documents. Excel 4.0 macros, or XLM macros, were first added to Excel in 1992 and allowed users to enter various commands into cells that are then executed to perform a task. While VBA macros were introduced in Excel 5.0, threat actors continue to use XLM macros twenty years later in malicious documents that download malware or perform other unwanted behavior. Malicious campaigns utilizing Excel 4.0 XLM macros include ones for malware, such as TrickBot, Qbot, Dridex, Zloader, and many more. Due to their continued abuse, Microsoft has been recommending users switch from and disable Excel 4.0 XLM macros for years in favor of VBA macros. This recommendation is because VBA macros support the Anti-malware Scan Interface (AMSI), which can be used by security software to scan macros for malicious behavior.

CAUSE OF ISSUE

Lack of Malware Protection

TYPE OF LOSS

System Compromise via Code Execution

The Telegraph exposes 10 TB database with subscriber info

TYPE OF LOSS

Loss of Sensitive Data

'The Telegraph', one of the UK's largest newspapers and online media outlets, has leaked 10 TB of data after failing to properly secure one of its databases. The exposed information includes internal logs, full subscriber names, email addresses, device info, URL requests, IP addresses, authentication tokens, and unique reader identifiers. Bob Diachenko, the researcher who discovered the unprotected dataset on September 14, 2021, has confirmed that at least 1,200 unencrypted contacts were accessible without a password at the time of his review. Notably, many of these cases concern registrant information of Apple News subscribers, also including passwords in plaintext form. The newspaper was contacted and warned about the exposure immediately, but it took them two days to eventually respond and secure the database.

ATTACK TYPE

Data Breach - Sensitive Data Exposure

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

Android October patch fixes three critical bugs, 41 flaws in total

ATTACK TYPE

Zero Day Vulnerability

Google has released the Android October security updates, addressing 41 vulnerabilities, all ranging between high and critical severity. On the 5th of each month, Google releases the complete security patch for the Android OS which contains both the framework and the vendor fixes for that month. As such, this update also incorporates fixes for the 10 vulnerabilities that were addressed in the Security patch level 2021-10-01. The high-severity flaws fixed this month concern denial of service, elevation of privilege, remote code execution, and information disclosure issues.

The three critical severity flaws in the set are tracked as: CVE-2021-0870: Remote code execution flaw in Android System, enabling a remote attacker to execute arbitrary code within the context of a privileged process. CVE-2020-11264: Critical flaw affecting Qualcomm's WLAN component, concerning the acceptance of non-EAPOL/WAPI frames from unauthorized peers received in the IPA exception path. CVE-2020-11301: Critical flaw affecting Qualcomm's WLAN component, concerning the acceptance of unencrypted (plaintext) frames on secure networks.

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Loss of Reputation and User Data

Bug in Popular WinRAR Software Could Let Attackers Hack Your Computer

A new security weakness has been disclosed in the WinRAR trialware file archiver utility for Windows that could be abused by a remote attacker to execute arbitrary code on targeted systems, underscoring how vulnerabilities in such software could become a gateway for a roster of attacks. Tracked as CVE-2021-35052, the bug impacts the trial version of the software running version 5.70. "This vulnerability allows an attacker to intercept and modify requests sent to the user of the application," Positive Technologies' Igor Sak-Sakovskiy said in a technical write-up. "This can be used to achieve remote code execution (RCE) on a victim's computer." The issue has since been addressed in WinRAR version 6.02 released on June 14, 2021.

ATTACK TYPE

Zero Day Vulnerability
Remote Code Execution

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

System Compromise via Code Execution

Slack contains an XSLeak vulnerability that de-anonymizes users

A security hole in the file-sharing feature of Slack enables malicious actors to identify users outside of the workforce messaging platform. Slack apparently has no plans to patch the flaw in its web application, saying users can prevent such attacks by ensuring everyone in their workspace is 'trusted.' Known as a cross-site leak (XSLeak), the vulnerability allows attackers to circumvent same-origin policy, a browser security feature that prevents tabs and frames of different domains from accessing each other's data.

ATTACK TYPE

Zero Day Vulnerability - Cross site Leakage

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Unauthorized Access to User Account

Data analytics firm exposed 2m Instagram and TikTok users' data

The cybersecurity team at Safety Detectives, led by Anurag Sen, discovered an unsecured ElasticSearch server belonging to IGBlade.com, a social media analytics site. The server stored scraped data of millions of social media users. The data was taken from TikTok and Instagram. Reportedly, at least 2.6 million user profiles have been exposed, equivalent to over 3.6 GB of data. The researchers dubbed it a shocking discovery since data scraping is banned on most social media websites, although it isn't illegal. Researchers claim that the data was left exposed without any encryption or password protection in place. The exposed data included: Full names, Usernames, location data, About details, Profile pictures, Phone numbers, Email addresses, Engagement rate metrics and Follower counts & following counts.

ATTACK TYPE

Data Breach - Sensitive Data Exposure

TYPE OF LOSS

Loss of PII Data

CAUSE OF ISSUE

Lack of Data Protection Policies & Methodologies

The University of Sunderland confirms Cyberattack

The University of Sunderland in the UK has taken its IT system down and is still unable to access online lectures following a cyberattack. The University of Sunderland is a public research institute with about 20,000 students, so the disruption from the cyber-attack affects many people. The first signs of disruption for the university's IT systems occurred on 14th October 2021 but remain widely impactful and unclear.

The attack appears to have taken down all telephone lines, the official website, and the primary email servers. Staff and students could not communicate over Microsoft Teams or the university's Canvas virtual learning environment (VLE), which can access coursework and feedback or submit assignments. The University campus remains open, but students are unable to use many on-site services, including printing and Wifi. Students could not access the library PCs, loan laptops, online journals, ebooks and other services.

ATTACK TYPE

Distributed DOS attack

CAUSE OF ISSUE

Lack of DDOS Protection and Firewall security

TYPE OF LOSS

Loss of Reputation and User Data

Olympus US systems hit by cyberattack

Olympus, a leading medical technology company, was forced to take down IT systems in the Americas (U.S., Canada, and Latin America) following a cyberattack that hit its network Sunday, October 10, 2021. "Upon detection of suspicious activity, we immediately mobilized a specialized response team including forensics experts, and we are currently working with the highest priority to resolve this issue," Olympus says in a statement published today, two days after the attack. The company did not disclose if customer or company data was accessed or stolen during the "potential cybersecurity incident," but said that it would provide new information regarding the attack as soon as it's available.

ATTACK TYPE

Unknown

CAUSE OF ISSUE

Lack of Security Measures

TYPE OF LOSS

Unknown

TYPE OF LOSS

System Compromise via Code Execution

MysterySnail attacks with Windows zero-day

Kaspersky technologies detected attacks with the use of an elevation of privilege exploit on multiple Microsoft Windows servers. The exploit had numerous debug strings from an older, publicly known exploit for vulnerability CVE-2016-3309, but closer analysis revealed that it was a zero-day. It was discovered that it was using a previously unknown vulnerability in the Win32k driver and exploitation relies heavily on a technique to leak the base addresses of kernel modules. Microsoft assigned CVE-2021-40449 to the use-after-free vulnerability in the Win32k kernel driver and it was patched on October 12, 2021, as a part of the October Patch Tuesday. Besides finding the zero-day in the wild, Kaspersky analyzed the malware payload used along with the zero-day exploit, and found that variants of the malware were detected in widespread espionage campaigns against IT companies, military/defense contractors, and diplomatic entities.

ATTACK TYPE

Zero Day Vulnerability - Code Execution

CAUSE OF ISSUE

Lack of Patch Management Solutions

Popular NPM library hijacked to install password-stealers, miners

Hackers hijacked the popular UA-Parser-JS NPM library, with millions of downloads a week, to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack. The UA-Parser-JS library is used to parse a browser's user agent to identify a visitor's browser, engine, OS, CPU, and Device type/model. On October 22nd, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices. According to the developer, his NPM account was hijacked and used to deploy the three malicious versions of the library.

ATTACK TYPE

Zero Day Vulnerability

CAUSE OF ISSUE

Lack of Patch Management Solutions

TYPE OF LOSS

Loss of User Data

SCUF Gaming store hacked to steal credit card info of 32,000 customers

SCUF Gaming International, a leading manufacturer of custom PC and console controllers, is notifying customers that its website was hacked in February to plant a malicious script used to steal their credit card information. SCUF Gaming customers were the victims of a web skimming (also known as e-Skimming, digital skimming, or Magecart) attack. Threat actors inject JavaScript-based scripts known as credit card skimmers (aka Magecart scripts, payment card skimmers, or web skimmers) into compromised online stores which allow them to harvest and steal customers's payment and personal info.

The malicious script was deployed on SCUF Gaming's online store after the attackers gained access to the company's backend on February 3rd using login credentials belonging to a third-party vendor. Two weeks later, on February 18th, SCUF was alerted by its payment processor of unusual activity linked to credit cards used on its web store. The payment skimmer was detected and removed one month later, on March 16th, following what the company calls "a rigorous investigation in partnership with third-party forensic specialists."

ATTACK TYPE	*CAUSE OF ISSUE*	*TYPE OF LOSS*
Data Breach – Sensitive Data Theft	Lack of Security Validation	Loss of PII data

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