THREATSPLOIT

ADVERSARY REPORT

BRISK INFOSEC

CYBER TRUST & ASSURANCE

EDITION 40

www.briskinfosec.com

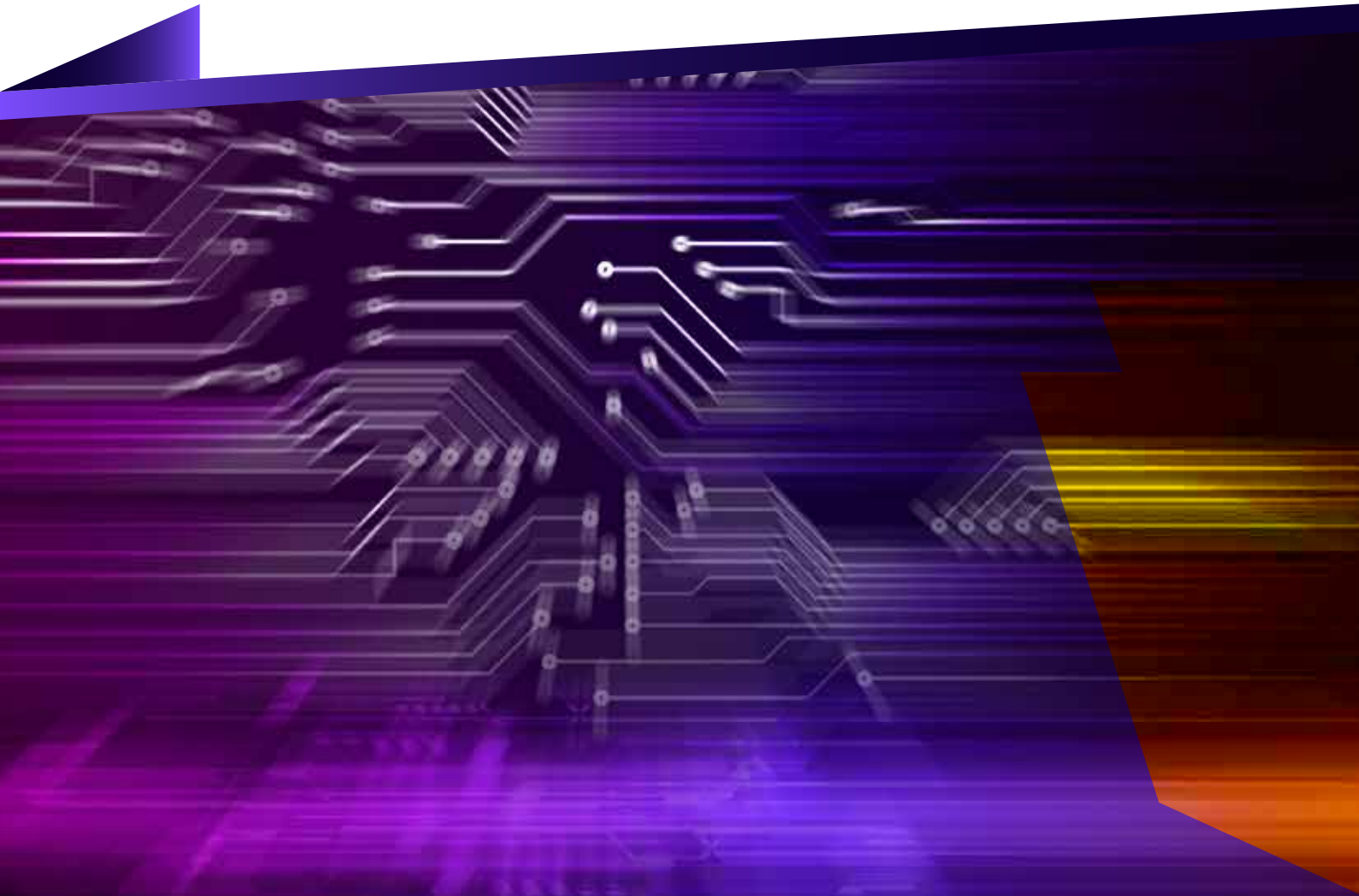
INTRODUCTION

Welcome to the Threatsploit Report of December 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

Philips, CISA Warn of Medical Device Product Security Flaws

Federal regulators and Philips this week issued advisories pertaining to several security vulnerabilities identified in certain patient monitoring and medical device interface products from the manufacturer. Exploitation could allow attackers to access patient data, launch denial of service attacks and more, they warn. The advisories pertain to vulnerabilities in Philips' Patient Information Center iX (PIC iX) and Efficia CM Series patient monitoring software and the company's IntelliBridge EC40 and EC80 systems - C.00.04 and prior versions, which are interfacing products to transfer data from point-of-care medical devices to hospitals' other information systems. Security researchers at Nozomi Networks identified and reported all of the vulnerabilities to the Cybersecurity and Infrastructure Security Agency, the advisories note. The products are used worldwide, CISA says.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
Sensitive Data

US, UK, Australia Issue Alert on Iranian APT Groups

Law enforcement and intelligence agencies in the U.S, U.K. and Australia have issued a joint advisory on unidentified Iran government-backed advanced persistent threat actors exploiting Fortinet and Microsoft Exchange ProxyShell vulnerabilities to attack organizations in their respective countries. The APT actors, the advisory says, do not target specific sectors. Their victims range across U.S. critical infrastructure sectors, including transportation and healthcare, as well as Australian organizations, it says. They exploit known vulnerabilities and can also use the access for "follow-on operations, such as data exfiltration or encryption, ransomware and extortion," the alert says.

Attack Type
Advanced Persistent Threat (APT) Attack

Cause of Issue
Lack of Secure Firewall Rules and Patch Management

Type of Loss
Source Code & Streamer User Data

SharkBot Trojan Targets Bank and Cryptocurrency Credentials

A newly identified banking Trojan dubbed SharkBot is now targeting banking and cryptocurrency service customers across the U.K., Italy and the U.S. through a sideloading campaign and/or a social engineering campaign that attempts to "initiate money transfers from the compromised devices via automatic transfer system techniques, bypassing multifactor authentication mechanisms such as strong customer authentication, according to the Cleafy threat intelligence research team. The malware has targeted customers of 22 different banks across the U.K. and Italy and five cryptocurrency services in the U.S., but it's not clear how many individual victims there have been or who's behind the campaign, the researchers says.

Attack Type
Malware Attack (Trojans)

Cause of Issue
Lack of Malware protection tools

Type of Loss
Sensitive Data

Intel Fixes 2 High-Severity Vulnerabilities

Chipmaker Intel has issued a security advisory for two high-severity vulnerabilities in the BIOS - basic input/output system - reference code in Intel processors that may allow privilege escalation attacks. The vulnerabilities, tracked as CVE-2021-0157 and CVE-2021-0158, have a high CVSS v3 score of 8.2. CVE-2021-0157 concerns the insufficient control flow management in the BIOS firmware for some Intel processors, and CVE-2021-0158 concerns improper input validation in the same firmware. Exploitation of both vulnerabilities can only be achieved with local access to the targeted systems, according to researchers Itai Liba and Assaf Carlsbad at security firm SentinelOne, Intel says.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise

MosesStaff Attacks Israeli Government, Other Organizations

Politically motivated hacker group MosesStaff has been targeting Israeli organizations with encryption attacks since September, according to researchers. The attackers state their primary motivate for the targeted campaigns "is to cause damage by leaking the stolen sensitive data and encrypting the victim networks, with no ransom demand," according to Check Point Research. As the ongoing attacks do not leverage zero-day vulnerabilities, "potential victims can protect themselves by immediately patching all publicly facing systems," the researchers say.

Attack Type
Data Breach – Sensitive Data Exposure

Cause of Issue
Lack of Data Protection Policies and Methodologies

Type of Loss
User Data Loss and Reputation Loss

Data of 5.9M RedDoorz Customers Leaked in Breach

Law enforcement and intelligence agencies in the U.S, U.K. and Australia have issued a joint advisory on unidentified Iran government-backed advanced persistent threat actors exploiting Fortinet and Microsoft Exchange ProxyShell vulnerabilities to attack organizations in their respective countries. The APT actors, the advisory says, do not target specific sectors. Their victims range across U.S. critical infrastructure sectors, including transportation and healthcare, as well as Australian organizations, it says. They exploit known vulnerabilities and can also use the access for "follow-on operations, such as data exfiltration or encryption, ransomware and extortion," the alert says.

Attack Type
Data Breach – Sensitive Data Exposure

Cause of Issue
Lack of Data Protection Policies and Methodologies

Type of Loss
User Data Loss and Reputation Loss

Zoom Patches Multiple Vulnerabilities

Cloud video conferencing provider Zoom has released patches for multiple vulnerabilities in its product that could have allowed criminals to intercept data from meetings and attack customer infrastructure. The vulnerability, tracked as CVE-2021-34417, fails to validate input sent in requests to set the network proxy password, which could lead to a remote command injection by a web portal administrator. The second vulnerability, tracked as CVE-2021-34422, is rated high with a CVSS score of 7.2 and affects Keybase Client for Windows that contains a path traversal vulnerability when checking the name of a file uploaded to a team folder. Another significant patch issued was for a Zoom Windows installation executable signature bypass flaw, which is rated as medium and has a CVSS score of 4.7. The vulnerability, tracked as CVE-2021-34420, affects all Zoom Client for Meetings for Windows before version 5.5.4.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise via Code Execution

Flaw Exposing Data of 44 Million Indian Investors Patched

A critical vulnerability in the Central Depository Services Ltd., or CDSL, which is India's largest securities depository, has been discovered and patched, according to researchers. Exploitation of the vulnerability could have potentially exposed sensitive information of 43.9 million investors in the country, note the researchers at cybersecurity consultancy firm CyberX9. The breach, they add, would have affected all Indian investors, who are mandated to have a KYC-compliant demat account that holds financial securities in electronic form. The exposed database included personal information of investors, such as full name, address, telephone number and email ID as well as highly sensitive data, such as Permanent Account Number or PAN, income and net worth, broker name, amount of annual income tax return filed and CDSL client ID, the researchers say. The exposed information dated back to 2005, they add. CDSL Ventures Ltd. took immediate action to mitigate the vulnerability and has worked proactively to address any other potential security issues as well, the organization told news platform Hindu Business Line.

Attack Type
Data Breach – Sensitive Data Exposure

Cause of Issue
Lack of Data Protection Policies and Methodologies

Type of Loss
User Data Loss and Reputation Loss

55 Patches, 6 Zero Days – Is There a Backlog at Microsoft?

Microsoft's November Patch Tuesday security update covers 55 security fixes, six of which are zero-day vulnerabilities, with two flaws actively exploited in the wild. One of the key vulnerabilities patched is Microsoft Exchange Server Remote Code Execution (CVE-2021-42321), which is rated as important by Microsoft because the attacker must be authenticated to be able to exploit the vulnerability. The CVE-2021-42321 vulnerability has a CVSS score of 8.8, and Microsoft has confirmed that it is being exploited in the wild. CVE-2021-42292 is also being actively exploited in the wild. This Microsoft Excel security feature bypass vulnerability has a CVSS score of 7.8, which puts it in the high-severity rating category. Breen says Microsoft does not offer any suggestion on what effect this vulnerability can have.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise via Code Execution

Hive Threat Group Attacks MediaMarktSaturn, Demands Ransom

MediaMarktSaturn Retail Group, a German multinational chain of stores, has confirmed to Information Security Media Group that it has suffered a ransomware attack. The attackers are demanding $50 million, according to a Tuesday report from Dutch media outlet RTL Nieuws, which is a huge drop from the $240 million ransom reported by news platform Bleeping Computer on Sunday. Bleeping Computer also attributed the attack to the Hive group.

Attack Type
Malware Attack – Ransomware

Cause of Issue
Lack of Malware Protection tools

Type of Loss
Loss of Sensitive user data

Server-side vulnerabilities in Concrete CMS put thousands of websites under threat

Multiple security vulnerabilities in a popular open source content management system (CMS) could allow a malicious attacker to gain full control of the underlying web server. The issues were discovered in Concrete CMS by researchers from Fortbridge, who detailed how two race condition vulnerabilities combined with the insecure use of the uniqid() function could allow an attacker with low privileges to achieve remote code execution (RCE).

Attack Type
Remote Code Execution

Cause of Issue
Lack of Security Patches

Type of Loss
Web Server Compromise

Microsoft fixes reflected XSS in Exchange Server

Microsoft has patched a reflected cross-site scripting (XSS) vulnerability in Exchange Server. Tracked as CVE-2021-41349, the flaw was unearthed by security researcher Rahul Maini and Harsh Jaiswal, application security engineers at Vimeo. The medium severity spoofing bug (CVSS score 6.5) has a low attack complexity, according to Microsoft, which published a security advisory on November 9 indicating that there was no evidence, as yet, of in-the-wild exploitation. Maini said the exploit would work on almost every unpatched Outlook Web App, on-premise instance. Microsoft has issued five software updates applicable for Exchange Server 2013, 2016, and 2019 that address the vulnerability.

Attack Type
Cross site Scripting

Cause of Issue
Lack of Secure Input Validation and Patches

Type of Loss
Mail Server Data Loss

Palo Alto GlobalProtect users urged to patch against critical vulnerability

Security researchers have discovered a high-impact vulnerability on some versions of the widely used Palo Alto GlobalProtect Firewall/VPN that leaves enterprise networks open to attack. The vulnerability (CVE 2021-3064; with a 'critical' CVSS score of 9.8) allows for unauthenticated remote code execution (RCE) on multiple versions of PAN-OS 8.1 prior to 8.1.17. Systems running PAN-OS versions 9.0, 9.1. 10.0, and 10.1 are immune but that still leaves thousands of older, internet-exposed systems open to attack. The security flaw was discovered by Randori, a red team-focused security consultancy, a year ago. Randori has since developed a working exploit that illustrates the scope for potential mischief. "If an attacker successfully exploits this vulnerability they gain a shell on the affected target, access sensitive configuration data, extract credentials, and more," the researchers said. "Once an attacker has control over the firewall, they will have visibility into the internal network and can proceed to move laterally."

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise

Apache Storm maintainers patch two pre-auth RCE vulnerabilities

Apache Storm, an open source real-time streaming data analytics platform, has patched two vulnerabilities that led to remote code execution (RCE). Discovered and reported by GitHub Security Lab, the bugs included a command injection vulnerability and an unsafe deserialization bug. The first of the two vulnerabilities was found in one of the functions of Nimbus, the principal component of Storm, which runs on top of a Thrift server. The function getTopologyHistory takes a username argument and concatenates it into a shell command without sanitizing it. An attacker can exploit the argument to send operating system commands to the Apache server.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise via Code Execution

Mozilla disables 'low usage' encryption feature to resolve Thunderbird HTTP/2 vulnerability

Mozilla has updated its Thunderbird email client to resolve an array of security flaws, including four high-severity web security vulnerabilities. The CVE-2021-38503 vulnerability meant that iframe sandbox rules were not correctly applied to XSLT stylesheets, potentially allowing a malicious iframe to "bypass restrictions such as executing scripts or navigating the top-level frame". The vulnerability – more details on which can be found on the Bugzilla bug tracker – was discovered by security researcher Armin Ebert. A more subtle but likewise high-impact vulnerability (CVE-2021-38507) creates a means to bypass the privacy and integrity protections offered by secure HTTPS connections. The seldom-used Opportunistic Encryption feature of HTTP/2 allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection – including being same-origin with unencrypted connections on port 80.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
Code Execution in Email client

Cisco patches critical bug trio in Policy Suite and ONT networking devices

Cisco has patched critical vulnerabilities in Policy Suite software and its Catalyst Passive Optical Network (PON) switches that could lead to the full compromise of the platform and devices. A vulnerability in the key-based SSH (Secure Shell) authentication mechanism of Cisco Policy Suite could allow an unauthenticated attacker to access an affected system as root, according to a security advisory issued on Wednesday (November 3). Tracked as CVE-2021-40119, the flaw commands a CVSS rating of 9.8, just a sliver off the maximum severity of 10.0.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise via SSH authentication

RCE vulnerability found in Sitecore enterprise CMS software

The researchers found that the software was vulnerable to a pre-authentication RCE attack due to insecure deserialization in the Report.ashx file. They discovered the vulnerability while probing Sitecore's attack surface during a client engagement. The vulnerability is pending a CVE number but is being tracked by the vendor as SC2021-003-499266. It impacts all Sitecore systems running affected versions, including single-instance and multi-instance environments, managed cloud environments, and all Sitecore server roles (content delivery, content editing, reporting, processing, etc), which are exposed to the internet. To remediate the problem, Assetnote advised users to "simply remove the Report.ashx file from /sitecore/shell/ClientBin/Reporting/", and pointed to Sitecore's security advisory. Sitecore has advised users to upgrade to version 9.0.0 or higher which protects against the vulnerability.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise via Code Execution

7 million Robinhood user email addresses for sale on hacker forum

The data for approximately 7 million Robinhood customers stolen in a recent data breach are being sold on a popular hacking forum and marketplace. Robinhood disclosed a data breach after one of its employees was hacked, and the threat actor used their account to access the information for approximately 7 million users through customer support systems. The data stolen during the attack included personal information for Robinhood users like email address, name, date of birth, and zip code. In addition to stealing the data, Robinhood stated that the hacker attempted to extort the company to prevent the data from being released.

Attack Type
Data Breach – Sensitive Data Exposure

Cause of Issue
Lack of Data Protection Policies and Methodologies

Type of Loss
Loss of Sensitive User Data

TikTok scammers tried hacking 125 targets that followed famous accounts, researchers find

More than 125 people and businesses associated with large TikTok accounts based around the world were targeted as part of a recent phishing campaign, according to research published on 16th November. Emails warned that targeted accounts were either in danger of being deleted for copyright violations or eligible for a verification badge. If victims replied to a message, attackers directed them to click a link to a WhatsApp chat, where a purported TikTok representative would confirm their accounts. While it remains unclear if any accounts were breached, the campaign is the latest to demonstrate how TikTok's popularity makes its most visible users targets for scammers.

Attack Type
Scamming – Phishing Campaign

Cause of Issue
Lack of security awarenees

Type of Loss
Loss of user account data

WordPress Sites Under Constant Attack

Last week, some 300 WordPress sites witnessed a wave of attacks, displaying fake encryption notices and asking for a ransom of 0.1 Bitcoin. Furthermore, these ransom demands induce a sense of urgency and panic by accompanying a countdown timer. This seems like a run of the mill ransomware attack. Researchers discovered that the websites were not encrypted. The threat actors simply altered an installed plugin, named Directorist, to show a ransom note and countdown. Thus, this is a fake ransomware attack.

Attack Type
Malware Attack – Ransomware

Cause of Issue
Lack of Malware Protection tools

Type of Loss
Loss of User Data

HTTP header smuggling attack against AWS API Gateway exposes systems to cache poisoning

A security researcher has explained how a weakness in the Amazon Web Services (AWS) API Gateway could be exploited via a HTTP header smuggling attack. Daniel Thatcher, a researcher and penetration tester at Intruder, said in a blog post dated November 10 that header smuggling – a relevantly new form of request smuggling technique – can be used to hide HTTP request headers from select servers, while keeping them visible to others. Tampering with the visibility of requests during a server chain can be lead to the successful deployment of malicious requests and request smuggling. Mismatching requests on back and frontend servers can potentially force the leak of data and secrets, as well as IP restriction bypass and cache poisoning.

Attack Type

Zero Day Vulnerability – HTTP Header smugglng

Cause of Issue

Lack of Secure Data Validation in API

Type of Loss

Loss of AWS API data

GoDaddy managed WordPress hosting service breach exposed 1.2m user profiles

The personal data more than 1.2 million GoDaddy customers was exposed after cybercriminals breached its WordPress hosting service, the company has admitted. In a statement filed with the US Securities and Exchange Commission, the internet infrastructure firm said it confirmed the breach on November 17 after detecting "suspicious activity" on its managed WordPress hosting environment. A subsequent incident response investigation by an external IT forensics firm uncovered evidence that the breach dates back more than two months, following an initial intrusion dating back to September 6. "Using a compromised password, an unauthorized third party accessed the provisioning system in our legacy code base for Managed WordPress," according to the domain registrar and web hosting firm.

Attack Type

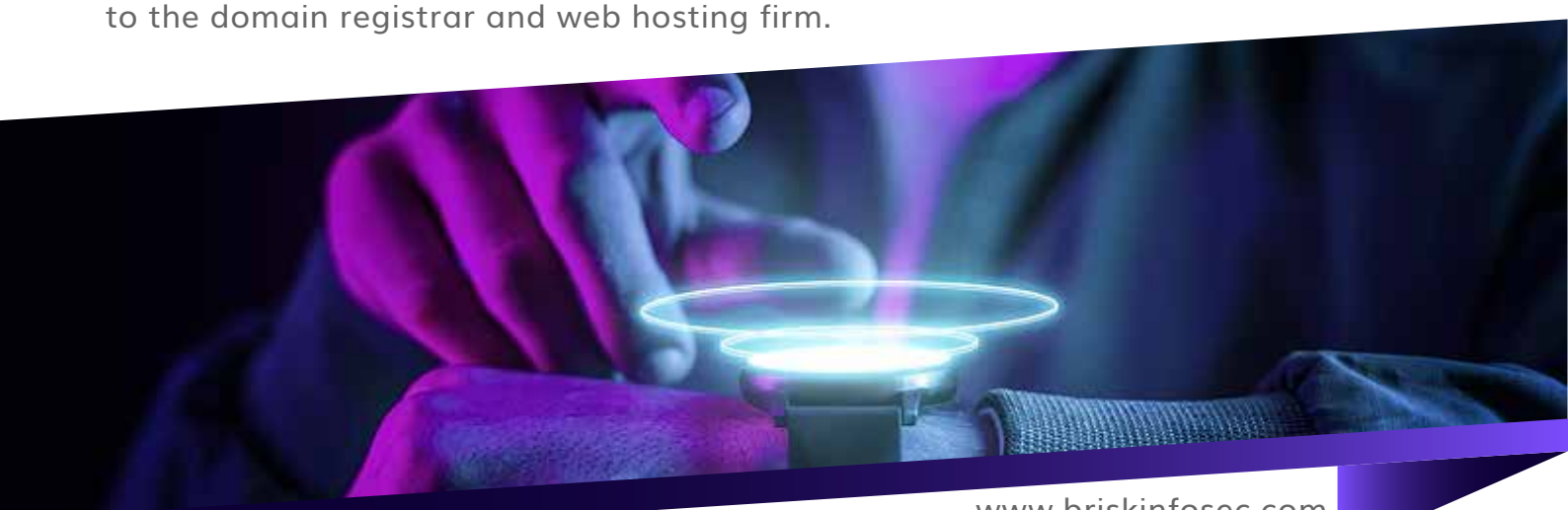
Data Breach – Sensitive Data Exposure

Cause of Issue

Lack of Data Protection Policies and Methodologies

Type of Loss

Loss of User Data and Reputation Loss



NUCLEUS:13 – Host of vulnerabilities shatter Nucelus TCP/IP stack defenses

Researchers have disclosed 13 vulnerabilities in the Nucleus TCP/IP stack, the worst of which can be used to remotely execute code. On November 9, Forescout Research Labs said the set of security flaws, collectively named NUCLEUS:13, were found with the assistance of Medigate Labs in Nucleus NET, the TCP/IP stack of the Nucleus Real-time Operating System (RTOS). In an advisory, the cybersecurity team said a total of 13 vulnerabilities have been found, ranging in severity from CVSS 5.3 to 9.8. The most severe vulnerability is CVE-2021-31886, a CVSS 9.8 buffer overflow flaw. Four other vulnerabilities also achieved high severity scores: CVE-2021-31346 (CVSS 8.2), an unchecked ICMP payload issue prompting data leaks and denial-of-service conditions; CVE-2021-31884 (CVSS 8.8), an out-of-bound read/write bug caused by errors in hostname definitions, and both CVE-2021-31887 and CVE-2021-31888 (CVSS 8.8), two FTP server validation command problems which could be used to trigger denial-of-service and RCE.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise and DOS attacks

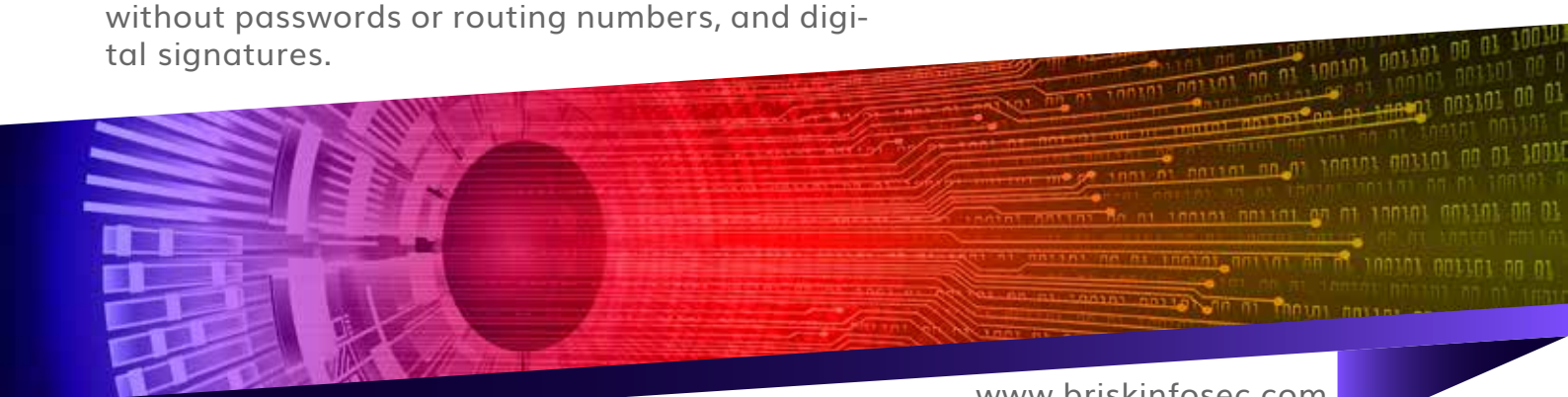
Data breach at US healthcare provider Viverant PT impacts more than 6,500 patients

A data breach at a physical therapy center based in the US has breached the personal data of more than 6,500 patients. Viverant PT, based in Minneapolis, Minnesota, said that the personally identifiable information (PII) of current and former patients and employees was affected in the breach. A wealth of healthcare information is reported to have been leaked, including patient names, addresses, dates of birth, Social Security numbers, driver's license numbers, and medical record numbers. Other potentially accessed data includes diagnostic or treatment information, payment card numbers with passwords or security codes, health insurance information, financial account numbers with or without passwords or routing numbers, and digital signatures.

Attack Type
Data Breach – Sensitive Data Exposure

Cause of Issue
Lack of Data Protection Policies and Methodologies

Type of Loss
Loss of Health Records



Eavesdropping Bugs in MediaTek Chips Affect 37% of All Smartphones and IoT Globally

Multiple security weaknesses have been disclosed in MediaTek system-on-chips (SoCs) that could have enabled a threat actor to elevate privileges and execute arbitrary code in the firmware of the audio processor, effectively allowing the attackers to carry out a "massive eavesdrop campaign" without the users' knowledge. Tracked as CVE-2021-0661, CVE-2021-0662, and CVE-2021-0663, the three security issues concern a heap-based buffer overflow in the audio DSP component that could be exploited to achieve elevated privileges. The flaws impact chipsets MT6779, MT6781, MT6785, MT6853, MT6853T, MT6873, MT6875, MT6877, MT6883, MT6885, MT6889, MT6891, MT6893, and MT8797 spanning across versions 9.0, 10.0, and 11.0 of Android.

Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise

APT C-23 Hackers Using New Android Spyware Variant to Target Middle East Users

A threat actor known for striking targets in the Middle East has evolved its Android spyware yet again with enhanced capabilities that allow it to be stealthier and more persistent while passing off as seemingly innocuous app updates to stay under the radar. Also known by the monikers VAMP, FrozenCell, GnatSpy, and Desert Scorpion, the mobile spyware has been a preferred tool of choice for the APT-C-23 threat group since at least 2017, with successive iterations featuring extended surveillance functionality to vacuum files, images, contacts and call logs, read notifications from messaging apps, record calls (including WhatsApp), and dismiss notifications from built-in Android security apps.

Attack Type
Malware Attack – Spyware

Cause of Issue
Lack of Malware Protection Tools

Type of Loss
Loss of Users Personal Data

Apple Sues Israel's NSO Group for Spying on iPhone Users With Pegasus Spyware

Apple has sued NSO Group and its parent company Q Cyber Technologies in a U.S. federal court holding it accountable for illegally targeting users with its Pegasus surveillance tool, marking yet another setback for the Israeli spyware vendor. In addition, the lawsuit seeks to permanently prevent the infamous hacker-for-hire company from breaking into any Apple software, services or devices. The iPhone maker, separately, also revealed its plans to notify targets of state-sponsored spyware attacks and has committed $10 million, as well as any monetary damages won as part of the lawsuit, to cybersurveillance research groups and advocates. To that end, the company intends to display a "Threat Notification" after the targeted users sign into appleid.apple[.]com, alongside sending an email and iMessage notification to the email addresses and phone numbers associated with the users' Apple IDs.

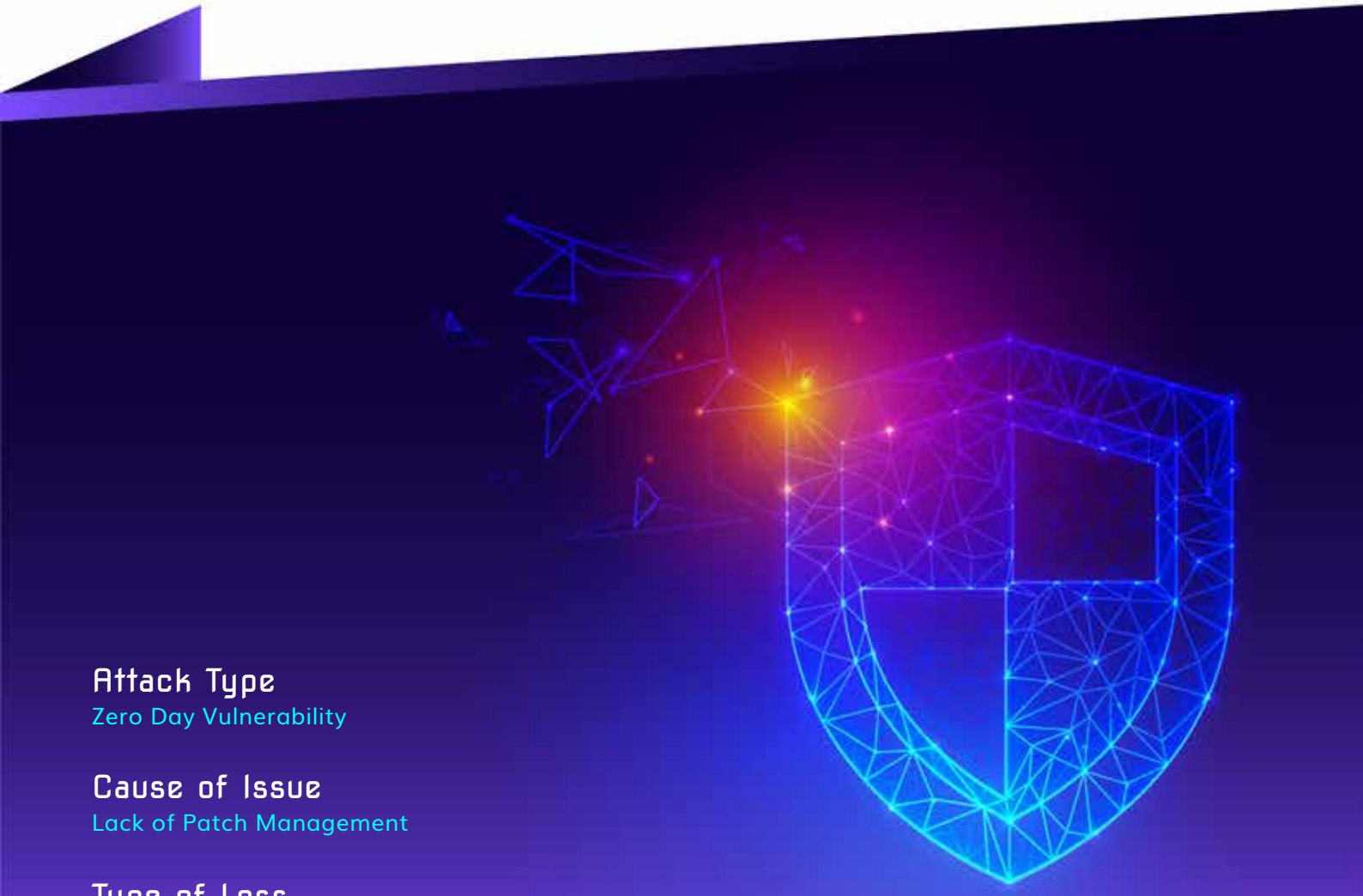
Attack Type
Malware Attack – Spyware

Cause of Issue
Lack of Malware Protection tools

Type of Loss
Loss of User Personal Data

VMware Warns of Newly Discovered Vulnerabilities in vSphere Web Client

VMware has shipped updates to address two security vulnerabilities in vCenter Server and Cloud Foundation that could be abused by a remote attacker to gain access to sensitive information. The more severe of the issues concerns an arbitrary file read vulnerability in the vSphere Web Client. Tracked as CVE-2021-21980, the bug has been rated 7.5 out of a maximum of 10 on the CVSS scoring system, and impacts vCenter Server versions 6.5 and 6.7. The second shortcoming remediated by VMware relates to an SSRF (Server-Side Request Forgery) vulnerability in the Virtual storage area network (vSAN) Web Client plug-in that could allow a malicious actor with network access to port 443 on vCenter Server to exploit the flaw by accessing an internal service or a URL request outside of the server. The company credited magiczero from SGLAB of Legendsec at Qi'anxin Group with discovering and reporting the flaw.



Attack Type
Zero Day Vulnerability

Cause of Issue
Lack of Patch Management

Type of Loss
System Compromise

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