Cyber Threat Investigations & Expert Services (CTIX) FLASH Wrap-Up

February 2023

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

CONTENTS

Executive Summary

The Ankura Cyber Threat Investigations and Expert Services (CTIX) FLASH Wrap-Up is a collection of high-level cyber intelligence summaries pertaining to current or emerging cyber events in February 2023, originally published in CTIX FLASH Updates throughout February. This publication includes malware threats, threat actor activity, and newly identified vulnerabilities impacting a wide range of industries and victims. The CTIX FLASH Update is a semi-weekly newsletter that provides a timely snapshot of cyber events, geared toward cyber professionals and end users with varying levels of technical knowledge. The events published in the FLASH typically occurred close in time to publication of the report.

To stay up to date on the latest cyber threat activity, sign up for our weekly newsletter: the Ankura CTIX FLASH Update.

MALWARE ACTIVITY

Russian Espionage Group Uses Go-Based Malware "Graphiron" to Target Ukrainian Organizations

Reported in the February 10th, 2023, FLASH Update

- "Graphiron", a new information-stealing malware, has recently been observed in attacks targeting an array of Ukrainian organizations. The attacks are being launched by the Russian espionage group Nodaria (aka UAC-0056), who has been active since at least March of 2021. Graphiron is written in the Golang programming language and is designed to "harvest a wide range of information from the infected computer, including system information, credentials, screenshots, and files." The earliest evidence of this malware is cited to be from October 2022 and is comprised of two stages: a downloader and a payload. The downloader checks for various malware analysis tools once executed, and if no tools are found, it connects to a hardcoded command-and-control (C2) server in order to download and decrypt the payload. Then, the payload is added to an autorun location for persistence. Researchers noted that the downloader makes just one (1) attempt to download and install the payload, meaning it won't make additional attempts if it fails or sends a heartbeat. Graphiron uses hardcoded file names designed to disguise themselves as Microsoft Office, such as "OfficeTemplate.exe" and "MicrosoftOfficeDashboard.exe". Graphiron is noted to have similarities to other malware used by the Nodaria group, including "GraphSteel" and "GrimPlant", and is constantly evolving its capabilities in order to evade defensive measures. Additional information on the Nodaria threat group as well as indicators of compromise (IOCs) can be viewed in Symantic's report linked below.
    - TheRecord: Graphiron Article
    - Symantic: Graphiron Report

Threat Actors Observed Using Legitimate Platform Geo Targetly in Phishing Campaigns

Reported in the February 14th, 2023, FLASH Update

- Detailed in a new report by Avanan, threat actors were recently observed geo-targeting websites through the platform Geo Targetly. This tactic is used to improve their phishing campaigns by sending customized, geo-specific content (typically by language and region) to different users in one phishing email. Geo Targetly is a legitimate platform that allows "advertisers to redirect users to pages and ads in their local markets" by determining the users' geolocation. These threat actors are utilizing a variant of the "spray-and-pray" technique, which is when an actor sends out a large volume of phishing emails and few are successful. The unique aspect in this campaign is that a large number of users are targeted at once and the content is always relevant and localized, which is being referred to as "spraying without the praying." The customization increases the likelihood of a user falling victim to the attack. In this campaign, a user will access a phishing link that will redirect them (using the legitimate platform) to a fraudulent login page that looks identical to the one it is impersonating and is based in the region the user is located in. Avanan researchers detailed that this is the first instance they have identified Geo Targetly being used and the campaign's method allows for a "fairly widespread attack." Geo Targetly has confirmed that they are aware threat actors are capitalizing on their platform but also argued that this method is not unusual. A Geo Targetly spokesperson claimed that the platform is a URL shortener similar to Bitly and smartURL, and that it is "common for hackers to hide the final destination URL behind a public URL-shortening domain." The spokesperson did confirm, however, that the platform "manually check[s] through URLs created in [their] system to identify such bad actors." CTIX will continue to monitor for different methodologies capitalizing on geo-targeting and provide details of new tactics as they become available.

- The Record: Geo Targetly Article
- Avanan: Geo Targetly Report

MortalKombat Ransomware and Laplas Clipper Malware Observed in New Campaign

Reported in the February 17th, 2023, FLASH Update

- A new financially motivated campaign that deploys the emerging "MortalKombat" ransomware and a Golang variant of the "Laplas" clipper malware has been identified. This campaign, which was first discovered in December 2022, has been observed targeting individuals as well as small and large organizations across primarily the United States, along with the United Kingdom, Turkey, and the Philippines. Researchers also noted that the currently unidentified actor responsible for the campaign has been observed "scanning the internet for victim machines with an exposed remote desktop protocol (RDP) port 3389" through an RDP crawler on a downloaded server. The attack chain begins with a phishing email that contains a malicious ZIP file and a cryptocurrency-themed lure impersonating a popular cryptocurrency payment gateway. The ZIP contains a BAT loader script that downloads an additional ZIP file from a controlled hosting server and executes the payload, which is either ransomware or the clipper malware. All evidence of the malicious files is then deleted. MortalKombat was first discovered in January 2023 and has been observed encrypting files on victim machines' filesystems (such as system, application, database, virtual machine files, and backup) as well as on remote locations mapped as logical drives. It is emphasized that there was no indication of wiper behavior or the deletion of large volume shadow copies in the observed instances. The researchers determined, through source code analysis, that MortalKombat has similarities to the Xorist ransomware family. Xorist first appeared in 2010 and has evolved by creating several variants through the use of ransomware builders. Laplas, which was first identified in November 2022, is a stealer malware that targets cryptocurrency users by "employing regular expressions to monitor the victim machine's clipboard for their cryptocurrency wallet address." A look-alike wallet address is created, and the victim's address is then overwritten. CTIX analysts urge users to stay vigilant when conducting cryptocurrency transactions and ensure their systems remain up to date with the latest security updates. A technical analysis as well as indicators of compromise (IOCs) can be viewed in the articles linked below.

    - The Hacker News: MortalKombat/Laplas Campaign Article
    - Cisco Talos: MortalKombat/Laplas Campaign Report

HardBit 2.0 Ransomware Urges Victims for Cyber Insurance Policy Details Prior to Establishing Ransom Amount

Reported in the February 21st, 2023, FLASH Update

- Researchers have observed samples of "HardBit 2.0" circulating throughout 2023 thus far and noted an interesting tactic identified in the latest campaign. HardBit, first discovered in October 2022, introduced version 2.0 in November 2022 and focuses on exfiltrating sensitive data upon gaining initial access to victims' networks and encrypting all data. The ransomware attempts to evade analysis by gathering data about the victim machine through web-enterprise management and Windows Management Instrumentation (WMI) functions. It then performs various techniques to lower the machine's security, such as deleting the Volume Shadow Copy Service (VSS) and the Windows backup utility, editing the boot configuration, disabling Windows Defender Antivirus features, and terminating services. Data is then encrypted and the ransom note is dropped. At this time, the operators behind the ransomware have not created a leak site to publish the stolen data

and double extortion does not appear to be in their playbook. In the dropped ransom note, HardBit urges victims to contact them through the Tox instant messaging platform or by email within forty-eight (48) hours of discovery. The threat actors also explain that they seek to negotiate with victims to reach a settlement rather than specifying a bitcoin amount within the ransom note. Victims with cyber insurance policies are urged to privately share their policy details during the negotiations in order to ensure HardBit's demands fall within their policies. The ransomware operators voice this tactic as benefiting both HardBit and the victim as opposed to the "poor multimillionaire insurers." If the ransom is not paid, HardBit often threatens additional attacks against the organization. CTIX recommends that victims of HardBit 2.0 engage an incident response firm to facilitate remediation and investigation of the incident. Indicators of compromise (IOCs) can be viewed in the report linked below.

- Bleeping Computer: HardBit 2.0 Article
- Varonis: HardBit 2.0 Report

Threat Actors Are Taking Advantage of ChatGPT's Popularity to Spread Windows and Android Malware

Reported in the February 24th, 2023, FLASH Update

- Threat actors have been observed spreading malware through ChatGPT-based phishing campaigns as the platform's popularity continues to rise. ChatGPT, a natural language processing chatbot that interacts with users' prompts to provide responses in a human-like text structure, was launched by OpenAI in November 2022 and had over 100 million users by January 2023. Though the platform has been widely used for legitimate purposes, researchers have identified various cases of ChatGPT-based lures and fraudulent phishing websites that focus on distributing malware and exfiltrating victims' credit card information. Some of these websites have been promoted through additional fraudulent sites impersonating OpenAI's social media page. Researchers detailed that one of the observed posts contained a link that leads victims to a typosquatted domain that disguises itself as the official ChatGPT website and promotes "ChatGPT for PC". This domain leads to a fraudulent OpenAI website that has a "Download for Windows" button that, when clicked, downloads a compressed file that contains Windows stealer malware. Several other stealer malware strains, including "Lumma Stealer" and "Aurora Stealer", as well as clipper malware were identified to be distributed by the phishing sites. Fake payment sites were also observed by researchers. Approximately fifty (50) malicious applications have been confirmed, as of February 22, 2023, capitalizing on the platform's icon and name to appear legitimate. Several malware families are involved in the malicious applications, such as adware, spyware, billing fraud, and more. Technical details regarding specific Android applications and phishing pages as well as indicators of compromise (IOCs) can be viewed in the report linked below.

  - Cyble: ChatGPT Campaigns Report

Unknown Threat Actors Target Government Entities Worldwide with "PureCrypter" Malware

Reported in the February 28th, 2023, FLASH Update

- Multiple government entities in North America and the Asia Pacific region have been targeted by currently unknown threat actors using the "PureCrypter" downloader malware. Through a Discord URL pointing to an encrypted ZIP archive as an initial attack vector, PureCryptor is used to install additional malware such as "Agent Tesla", "Eternity", and "Blackmoon" on the victim system. A

sample of the campaign's PureCrypter malware variant was analyzed by researchers, who determined that the malware leveraged Agent Tesla to connect to a compromised FTP server of a non-profit organization in Pakistan where exfiltrated data was being sent. The Agent Tesla malware allows threat actors to exfiltrate login credentials and further escalate attacks over time while avoiding detection by leveraging process injection, whereby the Agent Tesla executable code is injected into the process memory of a legitimate program. Agent Tesla also has the capability to screen capture and steal login credentials saved to a web browser or clipboard. CTIX analysts will continue to monitor attacks by this new threat actor and will provide updates accordingly.

- Bleeping Computer: PureCrypter Article
- The Hacker News: PureCrypter Article
- Menlo Security: PureCrypter Blog Post

THREAT ACTOR ACTIVITY

Threat Profile: NewsPenguin

Reported in the February 10th, 2023, FLASH Update

- A new threat organization has surfaced in the threat landscape and is actively targeting military and defense companies throughout Pakistan. Under the codename NewsPenguin, this group has launched an espionage campaign against Pakistan's Navy, using the upcoming Pakistan International Maritime Expo & Conference as a ploy in their phishing attacks. The name NewsPenguin originates from encryption keys within headers which were titled 'getlatestnews' and 'penguin'. Phishing emails from this campaign included a malicious Microsoft Office attachment with embedded macro-malware which, when enabled, would begin the infection chain, and compromise the user's device. Analysis of the malware code shows that it was written to gather and transmit confidential data from the user's system back to the threat actors. Indicators harvested from the malware showed geofencing capabilities (only executing certain code if the user's device originates from a Pakistani IP address), exfiltration endpoints, and domains registered around mid-2022; this suggests that the campaign was in planning for over six (6) months. While NewsPenguin has not been attributed to any one country, Pakistan has often been a target of Chinese state-actors over the past few years. CTIX is continuing to monitor this emerging threat group alongside other organizations throughout the world and will provide additional updates accordingly.
    - BlackBerry: NewsPenguin Report
    - TheRecord: News Penguin Article

Threat Profile: TA866

Reported in the February 14th, 2023, FLASH Update

- Another new threat organization has surfaced in the past months, an organization that has been targeting entities throughout the United States. The group is tracked as TA866 by security researchers and is financially-motivated based on observed tactics, techniques, and procedures (TTPs). TA866's first campaigns have been operating since October 2022 and are continuing to prosper well into 2023. This financially-motivated operation is dubbed "Screentime" and has been commonly targeting United States companies, alongside newly observed international targeting of German organizations. TA866 distributes phishing emails to their targets containing a variety of malicious tools including embedded URLs to Publisher and JavaScript files, Publisher attachments with macro-malware, and PDFs embedded with URLs to malicious JavaScript files. These phishing emails were distributed to over ten thousand individuals across over a thousand companies in the United States and Germany. Initially these phishing emails were observed targeting individuals two (2) to four (4) times per week but have slightly reduced in the new year with an overall higher volume of phishing emails. The malicious URLs, attachments, and tooling are not unique to TA866 and are available throughout underground forums and marketplaces. CTIX continues to monitor new activity originating from TA866 and will provide additional updates accordingly.
    - Proofpoint: TA866 Article

Threat Profile: WIP26

Reported in the February 17th, 2023, FLASH Update

- A cluster of threat actors classified as WIP26 have been conducting extensive cyberespionage campaigns against Middle Eastern telecommunications companies. WIP26 threat actors have

abused several cloud technologies (Google Firebase, Dropbox, Microsoft Azure) in previous attacks, covering malware delivery, data extraction, and command-and-control (C2) communications between the compromised asset(s) and threat actors. Intrusions during this campaign originate from socially engineered WhatsApp messages targeted at telecommunications employees. Within these messages, threat actors incorporate a seemingly trustworthy Dropbox URL claiming to contain documentation of poverty levels throughout the region. Alongside these documents, a masqueraded malware loader lives within the Wondershare PDFelement application. The malware loader deploys the CMD365 backdoor to the compromised system and functions as a C2 host from the enterprise's Microsoft 365 instance. CMDEmber is also deployed in parallel with CMD365, and is capable of gathering system information and exfiltrating it back to threat actor endpoints. WIP26 is predicted to continue adjusting tactics and techniques to masquerade their espionage efforts further in the coming months. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

- SentinelOne: WIP26 Article

Earth Yako Actors Target Japanese Education Sector

Reported in the February 21st, 2023, FLASH Update

- Threat actors from the Earth Yako APT group have been conducting a year-long targeting campaign against Japanese think tanks, researchers, and academic institutions. Earth Yako is a lesser-known threat group that has made a significant impact during this operation, showing their motivation lies with cyberespionage against their victims. The operation, dubbed Operation RestyLink/Enelink, began in January 2022 and has continuously targeted entities throughout the education sector with a variety of malicious tools and software. The standard point-of-entry for Operation RestyLink is spearphishing, attempting to persuade the user to download an embedded attachment which would eventually lead to the background download of one (1) or more malicious programs such as “MirrorKey” (DLL Loader), “TransBox” (Trojan), “PlugBox” (Trojan), “Dulload” (Generic), “PULink” (Dropper), and “ShellBox” (Stager). Incidents analyzed in this campaign include a Japanese academic center becoming compromised in March 2022 where MirrorKey and TransBox malware payloads were deployed. Months later in June, Earth Yako actors compromised researchers at another Japanese academic center and utilized MirrorKey and PlugBox payloads to further infect the compromised asset(s). Several additional incidents have occurred throughout this campaign, oftentimes for espionage purposes. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

  - TrendMicro: Earth Yako Article
  - Cyware: Earth Yako Article

Threat Profile: Clasiopa

Reported in the February 24th, 2023, FLASH Update

- Threat actors from a newly discovered threat organization, tracked as Clasiopa, have been targeting research laboratories throughout Asia. Little is known about this threat group, however, recent activity hints at threat actors utilizing brute force methods on public-facing infrastructure as their intrusion method. Additional tactics and techniques of Clasiopa includes checking IP addresses through a singular domain, attempting to disable anti-virus solutions, deployment of numerous malicious backdoors to gather file listings and exfiltrate data, and deletion of operating

system event logs. Malicious programs often deployed in Clasiopa include a customized remote access trojan (RAT) dubbed “Atharvan”, a modified “Lilith” RAT for remote command execution, a command-and-control (C2) tool called Thumbsender for file exfiltration, and customized proxy scripts. Clasiopa hasn’t been officially tied to any one nation, however based on some of the malicious programs the group utilizes and an encrypted ZIP archive with the password “iloveindea1998^_^” suggests an Indian influence. Furthermore, the command-and-control (C2) nodes utilized within the malware point to servers hosted out of South Korea, an uncommon location for these types of servers to communicate to. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

- Symantec: Clasiopa Article

Blind Eagle Actors Target Columbia

Reported in the February 28th, 2023, FLASH Update

- Threat actors from the Blind Eagle (APT-C-36) organization have been the source of an ongoing campaign against Columbian entities. Blind Eagle actors are known for their continued targeting of financial and government entities throughout Latin America. Ongoing since 2019, these threat actors have been distributing a variety of themed phishing emails attempting to compromise multiple users to gain access to company infrastructure. One instance observed by researchers demonstrated the use of fake tax documentation claiming to originate from Columbia's Directorate of National Taxes & Customs (DIAN). This type of lure has been used multiple times since the start of the campaign, as end-users often feel inclined to pay outstanding balances to tax agencies and uphold a good reputation with them. Embedded within these phishing emails was a fraudulent link to DIAN's official website that, once clicked, loaded a threat actor-controlled website. After downloading a fraudulent PDF document from a Discord CDN, additional code is executed from the malicious PDF and eventually installs AsyncRAT onto the compromised system. While Columbia appears to be the main target of this 4-year campaign, additional countries including Ecuador, Chile, and Spain have also been targeted. CTIX analysts continue to monitor threat activity throughout the threat landscape and will provide additional updates accordingly.
    - TheRecord: Blind Eagle Article
    - Blackberry: Blind Eagle Article

VULNERABILITIES

Toyota Patches Critical Vulnerability in Web-based Logistics Application

Reported in the February 10th, 2023, FLASH Update

- A vulnerability researcher named Eaton Zveare has published a report on his EatonWorks blog detailing how in October 2022 he was able to exploit a vulnerability in a Toyota employee logistics web application that allowed him to conduct a full takeover of the software anywhere it is used in the world. The software is known as the Global Supplier Preparation Information Management System (GSPIMS), and it allows Toyota employees and suppliers to coordinate logistics for parts, purchases, and projects. The vulnerability that Zveare exploited was in the GSPIMS application programming interface (API), and it allowed him to log in to GSPIMS as any corporate Toyota employee or supplier with only the knowledge of their company email address. Zveare alleges he was able to gain access to a directory of more than 14,000 users' "Toyota projects, documents, and user accounts, including user accounts of Toyota's external partners/suppliers." The access gave him full visibility into employee and supplier account details, as well as "confidential documents, projects, supplier rankings/comments, and more." In November 2022 Zveare reported the vulnerability to Toyota through its coordinated disclosure program, and the flaw was quickly patched. A Toyota spokesperson made a statement that there is no evidence that this vulnerability was ever exploited in-the-wild, and on his blog, Zveare applauded the company for having the "fastest and most effective" response to a security issue that he has ever reported. If exploited by threat actors, a flaw like this could cripple Toyota's operations and allow for creating rogue administrative user accounts, as well as stealing intellectual property and dropping devastating malware in the GSPIMS networks. The flaw was remediated, and there is no further action that needs to be taken by Toyota employees and suppliers. CTIX analysts will continue to report on interesting zero-day vulnerabilities, and technical details of Zveare's methods can be found in his blog post linked below.
    - The Record: Toyota Vulnerability Article
    - EatonWorks: Toyota Vulnerability Blog Post

Internet Analysis Finds Nearly 19,000 Vmware ESXi Servers Vulnerable to the ESXiArgs Ransomware Campaign

Reported in the February 14th, 2023, FLASH Update

- Several of the most respected cybersecurity research agencies around the world are continuing to warn organizations using VMware ESXi servers to patch an almost two (2) year old vulnerability to prevent being compromised by threat actors facilitating the "ESXiArgs" ransomware campaign. Researchers conducted internet-wide telemetry across more than seventy (70) services and protocols identifying 18,581 vulnerable internet-facing VMware ESXi servers. More than 3,800 organizations across the United States and Europe have already been compromised since the campaign started. VMware ESXi is a Virtual Machine Monitor (VMM) that installs directly onto a physical server, allowing access and control of the underlying resources. The years old vulnerability is tracked as CVE-2021-21974 and is a heap-overflow flaw in the ESXi OpenSLP service. Threat actors who gain access to the network segment of a vulnerable ESXi server facilitate their ransomware attack by exploiting this flaw to conduct remote-code execution (RCE). The campaign has been dubbed ESXiArgs due to the ransomware creating an additional file with the extension ".args" after encrypting a document, which contains the instructions for how to decrypt the encrypted document. In the first iteration of the ESXiArgs campaign, the ransomware encryption schema worked by checking the file size. If the file size was less than 128 MB, the entire file was

encrypted in one (1) MB increments. If the file was greater than 128 MB the encryptor script would calculate a "size_step", alternating between encrypting one (1) MB of data and skipping the calculated size_step. If a file was 4.5 GB in size, then the size_step would be forty-five (45), meaning that for every 1 MB of encrypted data, the script would skip 45 MB of the file. This size_step feature allowed the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) to create a ransomware decryptor script since, depending on the file size, there was already a large amount of unencrypted data. The decryptor script enabled victims to bring compromised servers back to a functional state while data restore from backup occurred in the background. Unfortunately, this led the actors behind the ESXiArgs campaign to modify the encryption script to encrypt 50% of all files over 128 MB, making them virtually unrecoverable and rendering the CISA decryptor useless for newly infected machines. To make matters worse, researchers have identified a relatively new ransomware strain known as "RansomExx2" that has been observed targeting Linux machines and exploiting vulnerable ESXi servers. At this time, it is unknown if the RansomExx2 attacks are being conducted by the same threat actors as the ESXiArgs campaign. To prevent exploitation, CTIX analysts recommend that all VMware ESXi administrators update their infrastructure immediately. In addition to patching, administrators should also remove the servers from the public-facing internet unless the service absolutely needs to be accessible, and ensure that there is a backup solution in place in the event of an ESXiArgs compromise. This campaign has yet to be attributed to a specific threat group, and CTIX analysts will continue to monitor the situation for new intelligence.

- The Record: CVE-2021-21974 Article
- Rapid7: CVE-2021-21974 Blog Post

CISA Adds Critical iOS Zero-day to the KEV

Reported in the February 17th, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has added an actively exploited critical Apple iOS zero-day vulnerability to their Known Exploited Vulnerabilities (KEV) catalog this week. If exploited, this flaw could allow malicious threat actors to execute arbitrary code on vulnerable devices. The vulnerability affects certain models of the iPhone, iPad Air, iPad Pro, and iPad Mini. This flaw, tracked as CVE 2023-23529, can be exploited by threat actors through social engineering attacks. An attacker could send the victim a phishing link via email, SMS, messaging applications, or embedded QR codes. If a threat actor was able to trick the victim into granting them initial access to the vulnerable device, they could then execute arbitrary code that downloads malware, giving the threat actor complete control of the device and the user's data. This vulnerability's presence on the KEV means that all non-military Federal Civilian Executive Branch (FCEB) agencies with vulnerable iOS devices have until March 7, 2023, to patch the flaw with iOS's latest update, or risk being fined by regulators. CTIX analysts recommend that any readers with vulnerable devices ensure that they are running the most recent secure version of iOS.

  - The Record: CVE 2023-23529 Article
  - Apple: CVE-203-23529 Advisory

Fortinet Patches Two Critical Vulnerabilities that Allow Attackers to Perform Arbitrary Code or Command Execution

Reported in the February 21st, 2023, FLASH Update

- Fortinet has patched two (2) critical vulnerabilities affecting two (2) of their network cybersecurity solutions. The first flaw, tracked as CVE-2022-39952, was given a 9.8/10 CVSS score and is an external control of file name or path vulnerability impacting the FortiNAC product, a network access control solution allowing Fortinet customers to manage network access to prevent threats. If exploited, an unauthenticated attacker could perform arbitrary write operations on a vulnerable system, allowing them to make configuration changes as well as move laterally across the network. The second flaw, tracked as CVE-2021-42756, was given a CVSS score of 9.3/10 and stems from multiple stack-based buffer overflow vulnerabilities impacting the FortiWeb product. FortiWeb is Fortinet's web application firewall (WAF) solution, which helps customers protect their internet-facing applications and APIs from web-based attacks like cross-site scripting (XSS), SQL injection, and distributed denial of service (DDoS) attacks. Threat actors could exploit this flaw by sending maliciously crafted HTTP requests, leading to arbitrary code execution. Fortinet has not provided manual mitigation techniques, and CTIX analysts recommend all network administrators responsible for vulnerable Fortinet solutions to patch their products immediately.
    - Bleeping Computer: Fortinet Vulnerabilities Article
    - FortiGuard: CVE-2022-39952 Advisory
    - FortiGuard: CVE-2021-42756 Advisory

CISA Adds Critical RCE IBM Vulnerability to the KEV Catalog

Reported in the February 24th, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has added an actively exploited critical IBM vulnerability to its known exploited vulnerabilities (KEV) catalog. The flaw, which was patched on January 18, 2023, is tracked as CVE-2022-47986 and affects the IBM Aspera Faspex file transfer tool. Aspera is extremely popular with large enterprises and organizations for transferring large datasets, like "genomics and biomedical research, media production, military signals intelligence, or financial services." In 2014, Aspera won an Emmy award for its work in the media production industry, enabling a boost in industry-wide workflows due to its ability to quickly transfer large media files. This vulnerability exploits an obsolete API call only present in Aspera Faspex versions 4.4.1 and earlier. A threat actor could make a maliciously crafted API call to a vulnerable instance of Faspex, which allows for remote code execution (RCE). This flaw received a CVSS score of 9.8/10 due to its active exploitation, as well as the low complexity of the exploit, coupled with the fact that attackers do not have to authenticate themselves prior to gaining initial access. At this time, Shodan searches indicate that more than 100 IBM Aspera Faspex servers are internet-exposed and may be vulnerable to exploitation. This vulnerability's presence on the CISA KEV mandates that all federal civilian executive branch (FCEB) agencies patch the flaw no later than March 14, 2023, or face financial penalties. This is not the first file transfer tool exploited to wreak havoc against major corporations. Just last week, the Russian-speaking ransomware-as-a-service (RaaS) group Clop claimed responsibility for exploiting the GoAnywhere MFT file-transfer tool, impacting one of the largest healthcare providers in the U.S., affecting more than 1 million patients and employees. CTIX analysts recommend that all organizations who depend on the IBM Aspera Faspex tool, immediately patch this vulnerability by updating their software to the most recent secure version.

- The Record: CVE-2022-47986 Article
- IBM: CVE-2022-47986 Patch Advisory
- CISA: KEV

WordPress Plugin for Real Estate Websites Contains Vulnerabilities Allowing for Website Takeover

Reported in the February 28th, 2023, FLASH Update

- Threat actors are actively exploiting two (2) vulnerabilities in a premium WordPress plugin/theme mainly used for real estate websites called Houzez. Claiming to serve more than 35,000 customers, ThemeForest's Houzez plugin offers simple tools that allow administrators to manage their agency's client listings, while providing content and a streamlined public-facing interface designed to provide the best customer service possible. Both vulnerabilities are privilege escalation flaws receiving CVSS scores of 9.8/10, making them both critical. The first vulnerability, tracked as CVE-2023-26540, stems from a security misconfiguration and affects all Houzez versions 2.7.1 or earlier. An unauthenticated threat actor could exploit this flaw to escalate their low-privilege accounts to high-privilege accounts, allowing them to ultimately take full control of the website. The second vulnerability, tracked as CVE-2023-26009, exists in Houzes' Login Register plugins in versions 2.6.3 and earlier, and also allows for a complete site takeover. The threat actors exploiting these flaws were observed uploading backdoors "capable of executing commands, injecting ads on the website, or redirecting traffic to other malicious sites." As stated, these vulnerabilities are under active-exploitation, and CTIX analysts recommend that all Houzez users ensure they are running the updated plugin to prevent exploitation.

    - Bleeping Computer: Houzez Plugins
    - PatchStack: Houzez Vulnerabilities Blog Post