ankura

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

December 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 December 2023, originally published in CTIX FLASH Updates throughout December. 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

Malicious Android Apps Used to Target Iranian Banks

Reported in the December 1st, 2023, FLASH Update

- An ongoing Android malware campaign targeting users of Iranian financial institutions has expanded to include new abilities to target an even greater number of people and prevent detection on compromised devices. The campaign consists of fake Android applications imitating the legitimate version of apps used by financial institutions. While originally only forty (40) Android apps had been discovered by researchers, a new report from Zimperium now states that more than 200 apps are connected to the malware campaign. These applications trick the device user into allowing escalated privileges before the malware abuses Android's accessibility services to harvest financial information, including bank account details, passwords, and credit card numbers. The latest findings suggest that these apps can also intercept SMS messages as well as prevent the uninstallation of the application so it may continue to harvest information. Additionally, greater use of public hosting services and command-and-control (C2) servers has allowed the threat actors to quickly adapt to changes in the environment to continue the attack, such as certain domains being taken down. Additionally, the threat actor has been observed launching phishing attacks against the financial institutions they are attempting to impersonate. These phishing campaigns utilize malicious webpages to impersonate the original website of the bank or crypto exchange. These combined campaigns against both the banks and their users have allowed the threat actors to capture information about the devices used by the victims and their financial account information all while exfiltrating the information to two (2) different Telegram channels. CTIX analysts will continue to monitor the evolution of this campaign.
    - The Hacker News: Malicious Android Apps Article
    - Github: Zimperium - Iranian-banking-malware IOCs

Bluetooth Compromise Coined "BLUFFS" Allows Attackers to Conduct Adversary-in-the-Middle Attacks

Reported in the December 5th, 2023, FLASH Update

- Researchers at EURECOM have developed six (6) new attack packages called "BLUFFS" that break the encryption of Bluetooth sessions. One of the original researchers stated that the attack targets previously unknown flaws in how the Bluetooth standard generates session keys. This is important as it means the Bluetooth standard itself has a flaw and is not limited to any specific hardware or software platform. Tracked as CVE-2023-24023, this issue impacts Bluetooth Core Specification 4.2, released in December 2014, through 5.4, released in February 2023. The issue works by exploiting the session key creation process to force the key created for the communication session to be abnormally short. This short length limits the possible combinations and thus allows the attacker to brute force the key so that decryption of the session is possible. After the initial compromised connection is made the threat actor may then cause the target device to establish a connection with the device in the middle to create a new encryption procedure using legacy encryption favorable to the attacker. While this does require the threat actor using this flaw to be within Bluetooth range of the two (2) communicating devices, it allows the attacker to then impersonate one (1) of the devices and begin an Adversary-in-the-Middle (AiTM) attack. EURECOM tested the various BLUFFS attacks they had devised on real world devices and discovered every device they tested was vulnerable to at least some of the attacks. This highlights the severity of the flaws found as it can be used on devices like Bluetooth enabled keyboards, mice, listening devices, and audio devices, presenting a large risk for a leak of data through an AiTM attack or for the attacker to inject malicious Bluetooth packets.
    - The Hacker News: BLUFFS Attack Article

New Linux Remote Access Trojan "Krasue" Targets Thai Telecom Sector

Reported in the December 8th, 2023, FLASH Update

- A newly discovered Remote Access Trojan (RAT) for Linux has been seen targeting telecommunications firms in Thailand as reported by Group-IB. Named RAT Krasue in reference to a Thai nocturnal spirit, this malware is quite dangerous to those networks it has infected. What is notable about this RAT is that it has been undetected on the infected networks since 2021, much longer than many campaigns are capable of. It has been able to accomplish this through a multitude of factors, some of which include UPX packing to both obfuscate the code and make the size of the malware smaller. It can also run itself as a background process and install additional rootkits based on the user's permissions. Additionally, it uses fake metadata to rename itself as various VMWare applications and programs to further avoid suspicion. RAT Krasue uses a designated IP as the master command-and-control (C2) server and uses the Real Time Streaming Protocol (RTSP) to send signals back to the C2 server without arousing suspicion. This protocol is typically used for applications such as video streaming to endpoint devices. One of the more novel approaches to hiding the malware has been to hijack the 'kill()' system call so it cannot be used against any of the malware processes and can be used to direct the rootkit via parameters passed to the 'kill()' call. This allows the threat actors to interact with the malware without raising alarm. Researchers also believe that the code for Krasue appears to be based on the rootkits Diamorphine, Suterusu, and Rooty. CTIX analysts will continue to monitor the effects of Krasue on telecommunication firms.
    - GROUP-IB: Krasue Article
    - The Hacker News: Krasue Article

New Trojan Targets macOS Devices

Reported in the December 12th, 2023, FLASH Update

- A new trojan has been discovered in-the-wild targeting macOS, distributed through pirated versions of business software. The malware begins by disguising itself as a program the user is trying to download, but once it is installed it creates a hidden proxy server within the system. This creates a backdoor into the network and also allows for traffic to be redirected through the infected device. This can allow the threat actor to utilize the victim's network and devices for a variety of purposes such as use in a botnet, redirecting internet traffic through the network to obfuscate illegal activity, or further install more malware onto the network. The threat actors have configured the trojan to use DNS-over-HTTPS, also known as DoH, to trick security services into thinking the traffic is non-malicious in nature. This allows the trojan to communicate to the command-and-control (C2) server without alerting the network owners. It is noted however that the C2 server is located at one location and does not appear to have backups, meaning that blocking that C2 server IP can permanently cripple the current version of the trojan. Another notable feature is that the trojan creates multiple files that it does not remove, allowing for easier identification of the trojan. This new trojan, albeit somewhat simple, is part of a wave that took off in 2019 of macOS trojans that appear to be targeting casual users to grow botnets in size and ability. CTIX analysts will continue to monitor the prevalence of botnet trojans and their ever-increasing target spread.
    - Dark Reading: Proxy Trojan Article
    - SecureList: Proxy Trojan Report

OilRig Group Deploys 3 New Malware Downloaders

Reported in the December 15th, 2023, FLASH Update

- Cybersecurity researchers have published reports showing that throughout 2022, OilRig (an Iranian state-sponsored threat actor also known as APT34, Crambus, Cobalt Gypsy, Hazel Sandstorm, and Helix Kitten) was observed deploying three (3) new downloader malware strains named ODAgent, OilCheck, and OilBooster, along with an updated version of a known downloader called SampleCheck5000 (SC5k), to maintain persistent access to victim organizations primarily in Israel. Active since 2014, OilRig Group mainly targets entities in the Middle East. The downloaders are notable for using legitimate cloud service APIs, like Microsoft Graph OneDrive, Outlook APIs, and Microsoft Office Exchange Web Services (EWS) API, for command-and-control (C2) and data exfiltration. This strategy aims to blend malicious activities with authentic network traffic, covering up the attack infrastructure. The targets of these attacks included entities in healthcare, manufacturing, and local government, many of which had been previously targeted by OilRig. Each downloader has unique characteristics. ODAgent, first detected in February 2022, is a C#/.NET downloader using the Microsoft OneDrive API for C2 communications. SampleCheck5000 interacts with a Microsoft Exchange mail account using the Office Exchange Web Services API. OilBooster, similar to ODAgent, uses the Microsoft OneDrive API, while OilCheck, like SampleCheck5000, uses Microsoft Graph API but for network communications. OilBooster and OilCheck also use the Microsoft Graph API to connect to a Microsoft Office 365 account, but they differ in their use of OneDrive and Outlook accounts for command retrieval and payload fetching.
    - The Hacker News: OilRig Group Article
    - WeLive Security: OilRig Report

QakBot Resurfaces in Phishing Campaign masquerading as IRS Employees

Reported in the December 19th, 2023, FLASH Update

- Qakbot, the botnet known for its phishing campaigns and injection into legitimate Windows processes to avoid detection, has reappeared in a new campaign targeting the hospitality industry. On December 15, 2023, Microsoft made a series of posts on X, formerly known as Twitter, describing their findings which involve a threat actor using PDFs to distribute the malware. This is despite Operation Duck Hunt, a multinational effort to bring down the Qakbot network and infrastructure, that was successfully executed earlier this year. Microsoft reported that threat actors are attempting to masquerade as IRS employees and distribute the Qakbot malware via malicious files through this new round of phishing. When the victim attempts to access the PDF, it will instead prompt them to download it for proper viewing which will actually download a ".msi" Windows installer file. Once executed, this file will install the Qakbot malware DLL onto the device. According to Microsoft, the DLL was generated on December 11th, which is the same day that the new phishing campaign began. Microsoft and other researchers have stated that there are some minor differences between the older versions of Qakbot and this latest attempt at its revival, indicating that someone is still working on this malware. One of the more notable changes is the use of AES to decrypt identified strings instead of XOR that was previously used. CTIX analysts will continue to monitor the situation with the new Qakbot campaign to identify any new developments and information.
    - The Hacker News: QakBot Article
    - Bleeping Computer: QakBot Article

Bogus F5 BIG-IP Update Embedded with Malware

Reported in the December 22nd, 2023, FLASH Update

- Israel has been victimized in a phishing campaign that has been delivering Windows and Linux data wipers to devices. The campaign is believed to be perpetrated by pro-Hamas hacktivists and

other Iranian-backed actors. The Israel Nation Cyber Directorate, a government organization dedicated to protecting Israeli cyber assets, released a report detailing how a phishing campaign impersonated a cloud security company. The email message describes a supposed zero-day vulnerability for F5 BIG-IP devices. It then urges the victim to download and install the update, which comes in the form of "F5Updater.exe" for Windows and "update.sh" for Linux. The Windows version of the executable creates a fake F5 security update with the F5 logo on the screen to further impersonate F5 and convince the victim that the software is legitimate. This pop up contains a clickable button that when clicked sends a message with device information to a Telegram channel after which it will attempt to wipe all data from the device. The Linux version works slightly differently, first trying to remove all users from the device using the Linux “wipe” command to remove all of the operating system files and the different partitions that may exist. After these commands are run, the device will restart which implements all of the changes made. BleepingComputer reports that the pro-Palestinian hacking group Handala has admitted responsibility for the attack campaign, but this remains unconfirmed as of December 21, 2023. CTIX analysts will continue to monitor newly discovered hacking campaigns that originate from the Middle East.

- Bleeping Computer: Fake F5 Update Article

THREAT ACTOR ACTIVITY

Iranian-linked Hackers Actively Exploiting PLCs Used in US Water Sector

Reported in the December 1st, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has released an advisory warning that hackers are targeting Water and Wastewater Systems (WWSs) facilities by exploiting their programmable logic controllers (PLCs), specifically Unitronics PLCs which are commonly used by many organizations in the water sector. PLCs are used in industrial settings to control and manage devices such as pumps, valves, pressure regulation, and the gathering of compliance data or the alerting of critical alarms to operations. A successful attack on PLCs located at a WWS could produce serious physical damages that could prevent the distribution of clean, portable water to the surrounding facility's community. The CISA advisory was linked to the recent attack on the Municipal Water Authority of Aliquippa in Pennsylvania which researchers have attributed to the Iranian-backed hacktivist known as Cyber Av3ngers who have been said to be attacking water and energy facilities using products from Israel. Following the attack, the water utility in Pennsylvania took systems offline and switched to manual operations to avoid risks to the municipality's water supply. Along with measures highlighted in the advisory, CTIX analysts recommend utilities enable multifactor authentication (MFA), change default passwords, install firewalls and VPNs where remote access is necessary, and disconnect PLCs from the open internet.
    - The Hacker News: Unitronics PLCs Article
    - Bleeping Computer: Unitronics PLCs Article
    - The Record: Unitronics PLCs Article

Unknown State-Sponsored Hackers XDSpy Targeting Russian Military-Industrial Companies

Reported in the December 5th, 2023, FLASH Update

- Researchers have recently observed a known state-controlled cyberespionage group targeting Russian military-industrial enterprises. XDSpy is the name of the group responsible for the recent attacks. They are threat actors that have been active since 2011 and mostly target countries in Eastern Europe and the Balkans. A report noted XDSpy hackers using phishing emails pretending to be researchers from an institute specializing in the design of nuclear weapons in order to gain access to the systems of the Russian metallurgical enterprise as well as a guided missile weapons development and production institute which proved to be unsuccessful. Some researchers see Russia as XDSpy's primary target but there has been limited first-hand visibility into attacks on Russia because of the lack of Western companies with sight of computer systems in the region, especially after many foreign cybersecurity firms left the country following the Ukraine invasion. XDSpy attacks on Russia have none the less been recorded by a number of researchers, with records of the threat actor having previously targeted the country's government, military, and financial institutions, along with their energy, research, and mining companies. This latest attack specifically has drawn unanimous agreement among researchers upon their attribution to XDSpy. Despite the long-standing presence of the threat actors, it has not been determined which country is backing the group. Their operational security sets them apart, having not made mistakes that compromise their identity or affiliation. The hackers don't operate a particularly complex toolkit, but their focus on obfuscation helps them evade security solutions and likely leads to above average rates of success. The CTIX team will continue to report on threat actor activity across the world.
    - The Record: XDSpy Article

Undocumented Threat Actors, AeroBlade, Targeting US Aerospace Organizations

Reported in the December 8th, 2023, FLASH Update

- A new, previously undocumented hacking group coined 'AeroBlade' was recently discovered targeting United States aerospace organizations in what are believed to be a series of attacks as part of a cyber espionage campaign. The group's origins are currently unknown, and it has yet to be determined whether the attacks were successful, but researchers speculate the purpose of mission was likely motivated by data theft or extortion. The attacks consisted of two (2) stages. The first stage began in September 2022 with the deployment of spear-phishing emails containing a document (docx) attachment with an embedded remote template injection to download the second-stage DOTM file. The second stage connects the attacker's command and control (C2) server by executing malicious VBA macros that enable a reverse shell on the target's system. During the first stage delivery mechanism, the victim opens a readable Microsoft Word document that appears legitimate while simultaneously dropping the next-stage payload that's executed once the victim manually clicks the "Enable Content" lure message. The second stage of the attacks didn't occur until July 2023, leading to the reverse shell payload consisting of a heavily obfuscated dynamic-link library (DLL) connecting to a hard-coded C2 server that transmited system information, including lists of all directories on the compromised computer, back to the attacker. The obfuscated DLL file features anti-analysis and anti-disassembly techniques that make detection and analysis difficult, while also skipping execution on sandboxed environments. Lastly, the payload established persistence on the system by means of a Task Scheduler, with a task named "WinUpdate2". Between the time of the two (2) attack phases, it was observed that the threat actor put a considerable amount of effort into the development of additional resources, indicating the evolution of their tools and growing sophistication capabilities of their attacks.
    - The Hacker News: AeroBlade Article
    - Bleeping Computer: AeroBlade Article
    - BlackBerry: AeroBlade Report

Lazarus Group Deploying Remote Access Trojans while Exploiting Log4j Vulnerabilities

Reported in the December 12th, 2023, FLASH Update

- A new global campaign being tracked as Operation Blacksmith has been tied back to the Lazarus Group, the notorious North-Korean-linked threat actors. The operation exploits security flaws in Log4j to install previously undocumented remote access trojans (RATs) onto victims' devices. Researchers have observed the use of three (3) DLang-based malware families so far including NineRAT, which uses Telegram to establish command-and-control (C2). The vulnerability these attacks are currently exploiting is being tracked as CVE-2021-44228, also known as Log4Shell, and the manufacturing, agriculture, and physical security sectors have been the main targets. Researchers have tied these latest tactics more specifically to the Lazarus sub-group Andariel (aka Onyx Sleet) who is often seen engaging in initial access, reconnaissance, and the establishment of longer-term access for Lazurus group activities. The NineRAT malware is used in these attacks as the main channel for interaction with infected endpoints and has the capability to send commands that help gather system information, upload, and download files, as well as uninstall and upgrade itself, all while using the legitimate Telegram messaging service for C2 communications that help enable detection evasion. The multitude of tools observed in use for Operation Blacksmith for backdoor access shows an overall high degree for persistent access. CTIX analysts will continue to monitor the ongoing operation for evolving developments.
    - The Hacker News: Operation Blacksmith Article
    - NIST: CVE-2021-44228 Advisory
    - NIST: CVE-2023-42793 Advisory

Russian-linked APT28 Using Israel-Hamas Lures to Target European Entities

Reported in the December 15th, 2023, FLASH Update

- The Russian nation-state threat actor APT28, also commonly known as FancyBear, TA422, Forest Blizzard, and many others, has recently been associated with a newly discovered campaign centered around Israel-Hamas lures to deliver a custom backdoor called HeadLace. The campaign is directed at thirteen (13) nations worldwide, including Hungary, Turkey, Australia Poland, Belgium, Ukraine, Germany, Azerbaijan, Saudi Arabia, Kazakhstan, Italy, Latvia, and Romania. The threat actors have been observed producing authentic documents as decoys created by academic, finance, and diplomatic centers, such as ones from the United Nations, the Bank of Israel, the U.S. Congressional Research Service, the European Parliament, a Ukrainian think tank, and an Azerbaijan-Belarus Intergovernmental Commission to target primarily European entities who have a "direct influence on the allocation of humanitarian aid." APT28's current campaign is one of a highly targeted nature where the nation-state threat actor's infrastructure is set up so that a singular instance of malware is only received by targets within a single country. A previous campaign by the threat actor in September 2023 used sensitive adult-themed lures while exploiting a Microsoft Outlook flaw to gain unauthorized account access to Exchange servers. Some of the attacks linked to the threat actor's current campaign using their custom HeadLace backdoor have employed RAR archives by exploiting a WinRAR vulnerability, tracked as CVE-2023-38831. The newer campaign shows a great deal of attention towards targeting distinctive victims, specifically individuals a part of the International Community (IC) who might have interests in emerging policy creation.
    - The Hacker News: APT28 Article
    - NIST: CVE-2023-38831 Advisory
    - NIST: CVE-2023-23397 Advisory

Attacks on Iranian Gas Stations Carried Out by Israel-Linked Attackers

Reported in the December 19th, 2023, FLASH Update

- It's been confirmed by Iranian authorities that gas stations throughout the country have experienced operational disruptions due to a cyberattack. Authorities have said that the attack took out 70% of the nation's gas stations, leaving 1,650 out of approximately 33,000 stations operational and the remaining stations operating their pumps manually. After Iran blamed the attacks on Israel and the US, an Israel-linked hacking group called Predatory Sparrow claimed responsibility calling it a retaliation for the aggressions of Iran and its allies in the region after supposedly sending out warnings the month prior. The hackers have previously claimed responsibility for two (2) successful attacks on the Iranian state-owned steel company and fuel distribution system, and Israeli media has reported before that it's believed these hackers are connected to Israeli military intelligence. Predatory Sparrow released a statement that despite having the capability to completely disrupt the entirety of gas stations across Iran, they conducted this attack in a controlled manner to ensure a portion of gas stations were left unharmed while limiting potential damages to emergency services. An increase in cyberattacks between Israel and Iran targeting each other have been observed in recent months as tensions have grown in Israel's war against the Palestinian militant group Hamas, signaling the prevalence cyber-warfare may play in evolving and future global conflicts.
    - Dark Reading: Predatory Sparrow Article
    - The Record: Predatory Sparrow Article

Indian Government Targeted in Operation RusticWeb Phishing Campaign

Reported in the December 22nd, 2023, FLASH Update

- The Indian government and defense sector have been targeted in Operation RusticWeb, a phishing campaign using Rust-based malware for intelligence gathering. First detected in October 2023, this campaign utilizes novel payloads and encrypted PowerShell commands to steal documents, with connections to the Pakistan-linked groups Transparent Tribe and SideCopy. SideCopy is involved in multiple campaigns delivering various known trojans like AllaKore RAT, Ares RAT, and DRat. The attacks, often initiated via phishing emails with malicious PDFs, leverage social-engineering to install malware that collects system information and files, sending them to an actor-owned command-and-control (C2) server. A different chain uses a PowerShell script and a Rust executable named "Cisco AnyConnect Web Helper," uploading data to a public file-sharing engine. This activity is linked to the nation-state actor DoNot Team, known for targeting individuals in Kashmir and India, using Android malware to infiltrate devices. The DoNot group continues to refine their techniques, posing a significant threat, especially in the Kashmir region. CTIX analysts will continue to report on the recent activity of state-sponsored and financially-motivated threat actors.
    - The Hacker News: Operation RusticWeb Article
    - SEQRITE: Operation RusticWeb Report

VULNERABILITIES

6th Google Chrome Zero-day Vulnerability Under Active Exploitation

Reported in the December 1st, 2023, FLASH Update

- Google Chrome has released urgent security updates in its latest patch that remediate seven (7) vulnerabilities, one of them being an actively-exploited critical zero-day bug. The zero-day vulnerability, tracked as CVE-2023-6345, is an integer overflow weakness existing in Chrome's Skia open-source 2D graphics library, an engine providing common APIs compatible with a wide variety of hardware and software. If successfully exploited, this flaw could allow threat actors that have compromised the renderer process to perform a sandbox escape via maliciously crafted files. The vulnerability was found by researchers from Google's own Threat Analysis Group (TAG) who indicated that the bug could be exploited by state-sponsored threat actors to deliver spyware to unsuspecting high-profile victims like journalists and politicians. The technical details of the exploit are currently being withheld to allow as many Chrome users as possible to update their vulnerable browsers, but Google has acknowledged that that a proof-of-concept (PoC) exploit exists in-the-wild. CTIX analysts will continue to monitor the fallout of this zero-day and may release an update if new information becomes public.
    - Bleeping Computer: CVE-2023-6345 Article
    - The Hacker News: CVE-2023-6345 Article
    - Google: Chrome Advisory

Healthcare Industry Under Attack by Ransomware Gangs Exploiting "Citrix Bleed" Vulnerability

Reported in the December 5th, 2023, FLASH Update

- The U.S. Department of Health and Human Services (HHS) is urging hospitals and healthcare facilities to patch an actively exploited critical vulnerability in Citrix Netscaler ADC and Netscaler Gateway known as Citrix Bleed. Netscaler monitors server health and optimizes resource utilization by allocating network and application traffic to adjacent servers. The flaw, tracked as CVE-2023-4966, is a sensitive information disclosure vulnerability affecting appliances configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA server. The flaw is already being exploited by ransomware actors to bypass password requirements and multifactor authentication (MFA), allowing for successful session hijacking of legitimate user sessions on Citrix NetScaler ADC and Gateway appliances. Currently, thousands of Citrix servers are vulnerable to exploitation, and many may have already been compromised. Although this flaw was patched in October 2023, it has been exploited by threat actors as a zero-day since at least August 2023. Center (HC3) team, the Health Sector Cybersecurity Coordination Center (HC3), has issued an urgent sector alert informing customers that they must immediately apply patches and upgrades to their systems to prevent exploitation. Multiple threat groups have already been identified as exploiting Citrix Bleed, and The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has published an advisory report warning that the flaw is already being exploited by threat actors leveraging the Lockbit 3.0 ransomware. CTIX analysts recommend that any administrators responsible for the affected appliances follow the patching and mitigation instructions in the HC3 alert linked below. Within the alert are also instructions for how healthcare organizations can investigate their networks to identify any indicators of compromise (IOCs) that may suggest their network has been compromised.
    - Bleeping Computer: Citrix Bleed Article
    - HC3: Citrix Bleed Sector Alert
    - Citrix: Citrix Bleed Advisory
    - CISA: Citrix Bleed Advisory

Known Adobe ColdFusion Vulnerability Still being Targeted in Unpatched Environments

Reported in the December 8th, 2023, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has notified that a known critical vulnerability in Adobe ColdFusion that was patched in March 2023 is still under active exploitation by threat actors attempting to gain access and control over government servers. Adobe ColdFusion is an application server and rapid scripting environment for developing and deploying web applications using ColdFusion Markup Language (CFML). The flaw, tracked as CVE-2023-26360, is an improper access control vulnerability which, if exploited, could allow threat actors to execute arbitrary code in the target environment. When the vulnerability was originally exploited as a zero-day in March, CISA did not disclose the name of the affected entity. In the December 2023 alert, America's Cyber Defense Agency warned that the flaw was being continuously exploited, and that in June 2023, the vulnerability led to the compromise of at least two (2) public-facing servers after threat actors successfully dropped malware payloads via "HTTP POST commands to the directory path associated with ColdFusion." Once they had gained access to the servers, threat actors attempted exfiltrating registry files as well as security account manager (SAM) information. Although the threat actors were able to gain access, the malicious activity was detected and blocked before they could exfiltrate data or move laterally across the network. This flaw was added to CISA's Known Exploited Vulnerabilities (KEV) catalog when it was originally exploited in March, meaning all Federal Civilian Executive Branch (FCEB) agencies are required to patch the bug. CTIX analysts recommend that any administrators responsible for Adobe ColdFusion servers patch this vulnerability immediately to prevent being compromised.
    - Bleeping Computer: CVE-2023-26360 Article
    - The Hacker News: CVE-2023-26360 Article
    - CISA: CVE-2023-26360 Advisory

Qlik Sense Actively Exploited to Deliver Ransomware

Reported in the December 12th, 2023, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two (2) actively exploited critical vulnerabilities affecting the Qlik Sense data analytics solution to the Known Exploited Vulnerabilities (KEV) catalog. Qlik Sense is an application heavily used by government organizations and large companies for visualizing and analyzing data, helping build interactive dashboards and reports, as well as extracting data from various sources. The first flaw, tracked as CVE-2023-41265 (CVSS 9.6/10), is an HTTP tunneling vulnerability, allowing threat actors to escalate their privileges and execute HTTP requests on the server hosting Qlik Sense. The second flaw, tracked as CVE-2023-41266 (CVSS 8.2/10), is a path traversal flaw allowing unauthenticated remote attackers to craft malicious HTTP requests to create anonymous sessions, permitting the attackers to send additional requests to other endpoints. These vulnerabilities are being chained together through exploitation to deliver ransomware and have already been used in a series of attacks by the Cactus ransomware group and several other threat actors. Qlik is very popular, having at least 40,000 users, and according to Shodan scans, approximately 6,000 instances are publicly exposed to the internet, many being U.S-based organizations. Since the application is used for data analytics, it is likely provided with both database and network access, making it a very high-value target for attackers. The vulnerabilities' presence on the KEV mandates that all Federal Civilian Executive Branch (FCEB) agencies must become compliant, applying patches no later than December 28, 2023. CTIX analysts urge that any administrators responsible for Qlik instances ensure that they are running a secure version. The servers hosting Qlik should also not be public-facing and accessible from outside of the network.
    - The Record: Qlik Sense Vulnerabilities Article
    - CISA: Qlik Sense Vulnerabilities Advisory

Russian State-sponsored Threat Group APT29 Targets Critical TeamCity Server Vulnerability

Reported in the December 15th, 2023, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other cybersecurity agencies have warned about a Russian hacking group APT29 targeting unpatched TeamCity servers since September 2023. APT29, linked to Russia's Foreign Intelligence Service (SVR), is known for its involvement in the SolarWinds supply-chain attack and breaches of multiple U.S. federal agencies. The threat actor has been exploiting a critical TeamCity vulnerability, tracked as CVE-2023-42793 (CVSS 9.8/10), which is an authentication bypass flaw allowing remote code execution without user interaction. Successful exploitation of this vulnerability enables attackers to compromise software developers' networks, potentially leading to further network breaches, lateral movement, and persistent access to compromised environments. The vulnerability also presents risks of software supply chain attacks via malicious code injection. Ransomware gangs and North Korean hacking groups, including Lazarus and Andariel, have also exploited this vulnerability. JetBrains, the developer of TeamCity, claims that over 98% of all TeamCity servers have been patched following the vulnerability disclosure. The vulnerability affects on-premises TeamCity instances, but the cloud version is not impacted. JetBrains has been actively contacting customers to encourage updates and has also provided a security patch for older TeamCity versions. CTIX analysts recommend that any administrators implementing TeamCity ensure that they are running the most up-to-date version to prevent exploitation.
    - CISA: CVE-2023-42793 Advisory
    - The Record: CVE-2023-42793 Article
    - Bleeping Computer: CVE-2023-42793 Article
    - The Hacker News: CVE-2023-42793 Article

Critical Apache Struts 2 Vulnerability Under Active Exploitation

Reported in the December 19th, 2023, FLASH Update

- A critical vulnerability in Apache Struts 2 is under active exploitation by treat actors attempting to achieve remote code execution (RCE). Apache Struts is a very popular Model-View-Controller (MVC) Java Framework used by developers to build enterprise web applications. The flaw, tracked as CVE-2023-50164 (CVSS: 9.8/10), was discovered by a researcher named Steven Seeley, who posted on X (Twitter) that a working proof-of-concept (PoC) exploit has already been made public. The bug is a path traversal vulnerability impacting how Struts handles file upload parameters. If successfully exploited, an attacker could gain complete control of affected systems by uploading a maliciously crafted file to the target environment, achieving arbitrary code execution. Apache Struts is a very popular framework for web application developers, and therefore is also a high-value target for attackers. This is not the first time Struts has been targeted, and in 2017 the notorious "Struts-shock" vulnerability was exploited to compromise the Equifax credit agency, exposing the credit information of nearly 150 million people. Although CVE-2023-50164 is just as destructive as the Struts-shock vulnerability, it is much harder to exploit, requiring highly sophisticated threat actors to accomplish exploitation. There is no workaround, and CTIX analysts recommend that any administrators and developers implementing Apache Strut ensure that their software has been patched.
    - Dark Reading: CVE-2023-50164 Article
    - Apache: CVE-2023-50164 Advisory

Google Patches Actively Exploited Zero-day Vulnerability in Chrome

Reported in the December 22nd, 2023, FLASH Update

- Google has released an emergency update for the Chrome browser to patch an actively-exploited high-severity zero-day vulnerability. The flaw, tracked as CVE-2023-7024, is a heap-based buffer overflow vulnerability in WebRTC allowing for potential exploitation targeting the Chrome desktop versions of Windows, Linux, and macOS systems. WebRTC is an open-source framework using real-time communication (RTC) for the web via JavaScript APIs. Successful exploitation could allow attackers to cause program crashes and execute arbitrary code with the privileges of the user. This vulnerability was identified and reported by Google's own Threat Analysis Group (TAG). Currently, the technical information regarding vulnerability and exploit are being withheld to allow as many Chrome and Chromium users as possible to patch their vulnerable browsers. Google's security advisory states that they are aware of an exploit for CVE-2023-7024 existing in the wild. CTIX analysts recommend that all users ensure their browsers are running the latest version to prevent exploitation.
    - Bleeping Computer: CVE-2023-7024 Article
    - The Hacker News: CVE-2023-7024 Article
    - The Record: CVE-2023-7024 Article
    - Google" CVE-2023-7024 Advisory