BRAINTRACE

THREAT ADVISORY REPORT

MARCH 4, 2021

braintrace™
INTELLIGENT CYBERSECURITY

TABLE OF CONTENTS

BACKGROUND

This report was created to update our clients on up-and-coming vulnerabilities and exploits that our security experts have discovered. Our team works diligently on researching threats and vulnerabilities to provide you with a safer network. If you have any questions, do not hesitate to contact us.

MINEBRIDGE TARGETING SECURITY RESEARCHERS

Information Security personnel are not immune from cyberattackers. Recently, the group behind Minebridge has been reported to have updated their malware in a campaign against security researchers.

Affected Systems

- Word

Vulnerability Overview

The campaign itself is not exactly new in that it attempts to deliver its payload via malware-laced Word documents sent via email. When downloaded, the malware embeds itself into the system via TeamViewer, which allows the attackers to download more software and payloads onto the target system.

When downloaded and opened, the malware displays a message that says, "file successfully converted to PDF." A decoy file is displayed that looks like a job resume. The code itself includes basic obfuscation techniques. Finger is used to download files, while CertUtil is used to decode data is received. Further exploitation of TeamViewer is used in a DLL side-loading. Coding changes were witnessed with the update in coding language to C++ as well.

This malware's different capabilities include remote code execution, file download, data exfiltration, self-updating and deletion, information gather, denial-of-service capabilities via process killing and shut down, and other activities.

Recommendation

The group attributed to this campaign has been seen in recent campaigns against financial institutions. As such, we recommend taking this threat with due seriousness. Defense-in-depth security postures, network and endpoint monitoring, antimalware, and EDR software are suitable precautions against this campaign style. Lastly, education regarding social engineering attackers is a must.

Reference

https://www.bankinfosecurity.com/updated-minebridge-rat-targets-security-researchers-a-16054

CNAME CLOAKING POSES THREAT TO WEB SECURITY AND PRIVACY

Web browsers have been making changes to prevent advertising technology companies from using third-party tracking. To mitigate this, advertising companies have been switching to a DNS technique called CNAME Cloaking that poses a threat to web security and privacy. In recent years, major web browsers, including Safari and Mozilla Firefox, have made countermeasures to prevent third-party tracking.

Affected Systems

- Several Popular Web Browsers

Vulnerability Overview

CNAME Cloaking is the technique of obscuring the distinction between first-party and third-party cookies, making tracking code appear to be first-party but is not. This could allow for leaking sensitive, private information, including location, emails, and full names, without the users' consent or knowledge. CNAME Cloaking uses the CNAME in their DNS configuration record to cloak websites that use first-party subdomains as an alias for the third-party tracking domains. This leads to the protection of blocking third-party cookies becoming ineffective. CNAME Cloaking also raises the concern of man-in-the-middle (MitM) attacks when the information is being sent to the tracker.

Recommendation

To Mitigate CNAME Cloaking, Firefox has an add-on, and Firefox 86 has Total Cookie Protection to prevent CNAME Cloaking.

Apple's iOS 14 and macOS Big Sur have safeguards in place within their Intelligent Tracking Protection (ITP) feature to protect against CNAME Cloaking.

Google has announced plans to block third-party cookies and trackers in Chrome in a new framework, called privacy sandbox, but is not expected to be released until 2022.

Reference

https://thehackernews.com/2021/02/online-trackers-increasingly-switching.html

ILLEGITIMATE FIREFOX BROWSER EXTENSION (FRIARFOX)

Advanced Persistent Threat (APT) actors are a group of trained hackers that usually have a vast amount of resources when it comes to hacking and can cause mass damage to the organizations they target. This article, an APT group known as TA413, has compromised a Firefox browser extension that allows the attackers to take over Gmail accounts.

Affected Systems

- Firefox browsers that have users logged in through their Gmail accounts.

Vulnerability Overview

TA413 targets users through phishing emails that contain a malicious URL that impersonated a YouTube link that, when clicked, will direct the user to an Adobe Flash Player Update that includes the malicious JavaScript Files.

To exploit Gmail accounts, there need to be some conditions met such as:

- Users logged into their Gmail account through the Firefox Browser
- User needs to access the browser extension through the Firefox Browser

There were various ways that the security researchers tested, and it came out to be that what was listed above would be the most effective way the attackers could take over a user's Gmail account.

Further research shows that the threat actors modified a legitimate browser extension known as Gmail Notifier but added malicious JS code and modified it to their liking.

Please see the full article provided in Reference for more details on this vulnerability, as well as a list of indicators of compromise.

Recommendation

Do not stay logged in through browser extensions when it comes to personal or business accounts. Implement phishing email education to employees regularly.

Reference

https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global

ADVANTECH WEB ACCESS/SCADA SOFTWARE PRIVILEGE ESCALATION VULNERABILITIES

Researcher Yuri Kramarz from Cisco Talos discovered multiple vulnerabilities in the Advantech WebAccess/SCADA software. This is a web-based SCADA solution used for developing IoT applications while transferring data to cloud applications. An attacker could exploit these vulnerabilities to extract data and elevate local privileges utilizing a variety of vectors.

Affected Systems

- Advantech WebAccess/SCADA v9.0.1

Vulnerability Overview

Below is a brief list of the vulnerabilities and descriptions:

CVE-2020-13550
Installation local file inclusion
This vulnerability exists in the installation functionality. A specially crafted application can lead to data disclosure when an attacker sends an authenticated HTTP request.

CVE-2020-13551
Privilege escalation via PostgreSQL executable
Any user on the system can replace binary located in the default installation on the PostgreSQL service to execute code with NT SYSTEM user privilege.

CVE-2020-13552
Multiple services allowing privilege escalation
This vulnerability allows an authenticated user to replace binary located in the default location to execute code with NT SYSTEM user privilege. You can either replace libraries loaded from the folder where service executables are or replace service binary.

CVE-2020-13553
Privilege escalation via Node.js script source
In the default dashboard process, users logging in will cause Node.Js scripts to start. By default, everyone will have permission to write to the startServerByServerConfig.Js file. Appending JavaScript code to the source will result in command execution.

CVE-2020-13554
Run Key Privilege Escalation in webvrpcs
This vulnerability points out the registry keys that reference binaries can be exploited by an attacker that would lead to escalated privileges when a new user logs in.

CVE-2020-13555
COM Server Application Privilege Escalation
COM Class Identifiers used by the Advantech WebAccess/SCADA references LocalServer32 and InprocServer32 with weak permissions. When invoked by higher privilege users, this can lead to privilege escalation.

Recommendation

No patches are available from the vendor at the moment. However, please keep a watch for patches from the vendor for the noted issues. Also, employ network segmentation and monitoring where possible.

Reference

https://blog.talosintelligence.com/2021/02/advantech-web-access-scada.html?&web_view=true

INCREASE IN QUICKBOOKS FILE DATA THEFT

QuickBooks is accounting software used by small and medium-sized businesses. Intuit creates this software. It is used to track invoices, manage bills, expenses, and keep track of profits and losses. ThreatLocker researchers published that they have noticed higher numbers of cyber-attacks recently. Attackers use a mixture of social engineering and phishing email attacks to access the victim's private data.

Affected Systems

- QuickBooks

Vulnerability Overview

Malicious attackers use social engineering to deliver malware that antiviruses cannot detect. Another option that they use to execute their attacks is a spear-phishing attack. They use malicious emails with the PowerShell commands contained in infected documents. When a file is downloaded, code will transfer QuickBooks files to the hacker's server.

Recommendation

It is recommended to follow proper cybersecurity steps. It is essential to be informed about phishing attacks. ThreatLocker advised that QuickBooks users should make sure that file permissions are not set on "Everyone." This step should mitigate exposure. Check Database Server Manager and make sure that privileges are appropriately set.

Reference

https://thehackernews.com/2021/02/experts-warns-of-notable-increase-in.html

T-MOBILE DISCLOSES DATA BREACH

In the last four years, T-Mobile was a victim of five data breaches. Each time, the breach was disclosed after bad actors already gained access to its customers' private data. This time hackers used a SIM swap type of attack. This type of attack exposes all personal identification data of the customers. Some of the breached data were their clients' names, SSN, addresses, emails, date of birth, type of the plan they used, PINs, and security questions.

Affected Systems

- T-Mobile

Vulnerability Overview

SIM swap allows malicious actors to control the victim's phone number through social engineering or bribing T-Mobile employees to follow their instructions. Hackers can bypass multifactor authentication

(MFA) since they will receive calls and messages directed to the victim's phone number. They are also able to access security credentials.

Recommendation

If you are a user of T-Mobile services, it is recommended that you change your password, PIN, and security questions and answers on your account. T-Mobile, in their announcement, mentioned that they are offering their customers free services for credit monitoring and identity theft detection.

Patch URL

https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping

Reference

https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/

MICROSOFT PUBLISHED CODEQL QUERIES TO FIGHT ATTACKS LIKE SOLARWINDS

SolarWinds' Orion platform was exposed to a supply-chain attack in December 2020. The full consequences of this attack are still unknown. To help cybersecurity experts and affected companies, Microsoft has developed CodeQL queries. By using this analysis engine, organizations can scan their source code for any malicious indicators of supply-chain attack. Microsoft was one of the companies that were affected by the recent SolarWinds attack.

Affected Systems

- Microsoft

Vulnerability Overview

Supply-chain attacks allow bad actors remote access to the victim's system, among many possible consequences. Microsoft released a public CodeQL query that will help users of the SolarWinds program scan their code and make sure that they have not been affected by the known IOCs. CodeQL is a semantic code analysis engine. CodeQL will allow the scanning of multiple malicious implants. Some of them are "time-bomb" functionality, command and control communication, Windows APIs found in the backdoor, and modified FNV-1A hash.

Recommendation

It is recommended to use CodeQL queries to ensure that systems were not affected by the supply-chain attack.

Patch URL

https://securitylab.github.com/tools/codeql

Reference

https://www.bleepingcomputer.com/news/security/microsoft-shares-codeql-queries-to-scan-code-for-solarwinds-like-implants/

ROCKWELL AUTOMATION LOGIX CONTROLLER CRITICAL VULNERABILITY

In a collective effort, researchers from Claroty, Kaspersky, and Soonchunhyang University were able to help identify a critical vulnerability in the integrity of Rockwell's Logix software. This vulnerability affects RSLogix 5000: v16 - v20 and Studio 5000 Logix Designer: v21+ and affects about 17 different Rockwell Logix Controller products. This massive critical vulnerability can allow attackers to upload malicious code to the controller, download sensitive data, or even install new firmware. This vulnerability has a score of 10 on the CVSS v3 scale.

Affected Systems

- CompactLogix 1768
- CompactLogix 1769
- CompactLogix 5370
- CompactLogix 5380
- CompactLogix 5480
- ControlLogix 5550
- ControlLogix 5560
- ControlLogix 5570
- ControlLogix 5580
- DriveLogix 5560
- DriveLogix 5730
- DriveLogix 1794-L34
- Compact GuardLogix 5370
- Compact GuardLogix 5380
- GuardLogix 5570
- GuardLogix 5580
- SoftLogix 5800

Vulnerability Overview

As covered by7 CVE-2021-22681, the Logix software used a key to verify communication like many devices in the world. This vulnerability is caused by the lack of protection of that key, allowing an unauthenticated attacker to bypass the verification control and authenticate with Logix controllers.

Recommendation

It's recommended to deploy proper network segmentation and use a firewall in necessary places. It is also recommended to put the controller's mode switch to "run" mode if applicable.

Reference

https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03

RYUK RANSOMWARE NOW SELF-SPREADS TO OTHER WINDOWS LAN DEVICES

There is a new version of Ryuk ransomware with worm-like capabilities. Ryuk is now capable of spreading to other devices on the original victim’s network. The group behind Ryuk operates as a Ransomware-as-a-Service (RaaS) that began in 2018. It is estimated this group made $150 million last year, $34 million from just one victim alone.

Affected Systems

- Machines with RPC accesses.

Vulnerability Overview

The French National cybersecurity agency in early 2021 came across while investigating a new variant of ransomware that they had not seen before. This variant looks and acts like traditional ransomware with one significant additive. This new version of Ryuk has worm-like capabilities and can spread to other devices within the victim network. When the victim launches the variant, it will immediately begin attacking the host system and making its way through every reachable system through which RPC Windows accesses are possible.

To propagate itself over the network, the ransomware will list all the IP addresses in the local ARP cache and send what will look like WOL (Wake on LAN) packets to each of the devices. It will then mount all the sharing resources found and encrypt the contents.

Recommendation

Keeping your systems updated and all patches current, keeping current backups of data and that they are current, and making sure the antimalware is current and in place are good recommendations to prevent ransomware infections. Refrain from opening any suspicious-looking emails, attachments, or clicking on any links that look suspicious as well.

This can be blocked from attacking other hosts by changing the privileged domain account's passwords for propagation to other hosts. If an attack from this version of ransomware were to occur, this would contain/limit the propagation.

Reference

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-now-self-spreads-to-other-windows-lan-devices/

APPLEJEUS CRYPTOJACKING MALWARE

North Korean cryptojacking malware AppleJeus has been used to target several countries and regions, including the United States. There are seven variants of the malware that are currently active. AppleJeus was first seen in 2018, with the latest version being discovered in late 2020. AppleJeus is disguised as a legitimate cryptocurrency trading platform to trick users into downloading the malicious application. The threat actors have also been seen using other methods to trick users into downloading malicious applications, such as phishing and social engineering techniques.

Affected Systems

- All Systems

Vulnerability Overview

The first three versions of AppleJeus are trojanized versions of legitimate cryptocurrency applications from Celas Trade Pro, JMT Trading, and Union Crypto. The threat actors used phishing emails of the companies with links to a fake website with links download the malicious application for Windows and Mac. The three trojanized applications' code is very similar except for the file names and location of the plist files in the script.

The other four versions are marketed and distributed by companies that appear legitimate cryptocurrency platforms but are fake. The fake companies include Kupay Wallet, CoinGoTrade, Dorusio, and Ants2Whale. All of their websites seem to be real companies but have grammatical errors. The websites also include downloadable files for the malicious cryptocurrency application, except for the Ant2Whale version. To download the malicious application for Ants2Whale, the site instructs the user to contact an administrator to receive the downloadable application. The scripts from the versions are similar with few differences.

For a full list of indicators for AppleJeus, please refer to the reference article.

Recommendation

It is recommended to verify the source of cryptocurrency-related applications before downloading and using them. For a complete list of mitigations, please refer to the reference article.

Reference

https://us-cert.cisa.gov/ncas/alerts/aa21-048a

NORTH KOREAN HACKERS TARGETING DEFENSE FIRMS WITH THREATNEEDLE MALWARE

A North Korean state-sponsored hacking group has been tied to an ongoing campaign to retrieve classified information from various defense industry departments. The Lazarus Group has been attributed with sending out COVID-themed emails in hopes that they will be opened, and the attachments embedded with ThreatNeedle malware downloaded dubbed ThreatNeedle.

Affected Systems

- Email's sent with a Microsoft Word document attachment included.

Vulnerability Overview

Using a spear-phishing attack campaign, the Lazarus Group sends out COVID-themed emails with a Word document attached to the email. When the user opens the infected document, the ThreatNeedle malware will begin running macro code to download and execute additional payloads on the system. ThreatNeedle will continue to embed itself inside, finding a backdoor for reconnaissance and deploying the malware for oblique movement, and start the exfiltration of data from the host system.

Once ThreatNeedle is fully installed into the infected system, it will take full control of the device it has attacked. It takes control using a credential harvesting tool called Responder. What this means is ThreatNeedle will be able to do anything from manipulating files to executing received commands. The hackers can even configure an Apache web server and use the router as a proxy between the two segments, making it so they could get data from the machines, which was otherwise unable to do.

The Lazarus Group has had ties in recent years to attacks on financial institutions and cryptocurrency businesses. This group has also been held responsible for the 2017 WannaCry ransomware campaign and Operation Blockbuster in 2014. In the early 2020's they have started their focus on aggressively attacking the defense industry, and ThreatNeedle is actively being used in the attacks towards defense firms.

Recommendation

Make sure all systems are up to date with the latest updates and security patches. This includes virus, malware, and spyware protection. Implementing multifactor authentication wherever it is possible is another excellent precautionary measure. Confirming an email before you click on an embedded link or attachment will prevent malicious activity from entering into the systems.

Reference

https://thehackernews.com/2021/02/north-korean-hackers-targeting-defense.html

VMWARE HAS REMEDIATED A HIGH SEVERITY FLAW IN DEFAULT VERSIONS OF VCENTER

VMware has announced that they have come up with a patch for their most recent high severity vulnerability in their vCenter products. This vulnerability almost scored a perfect score at 9.8 level severity. This vulnerability was found by the researcher Mikhail Klyuchnikov at the security firm Positive Technologies. This vulnerability is very dangerous because it allows for arbitrary remote code execution to be unleashed on the vulnerable server.

Affected Systems

- VMware vCenter server management platform.

Vulnerability Overview

This vulnerability involves an attacker executing arbitrary code remotely when they have access to port 443 on the victim server. The attack is not very sophisticated, and it does not require any interaction with users.

Recommendation

Upgrade vCenter server to versions 6.5 U3n, 6.7 U3l, or 7.0 U1c.

Patch URL

https://kb.vmware.com/s/article/82374

Reference

https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/

IBM ISSUES PATCHES FOR JAVA RUNTIME, PLANNING ANALYTICS WORKSPACE, AND KENEXA LMS

This week IBM has released security patches that have been designed to resolve the various high-medium vulnerabilities that the tech giant has been facing. These vulnerabilities impact Java Runtime, IBM Planning Analytics, and Kenexa. The vulnerabilities were first noted back in 2020 and until now did not have a resolution or patch.

Affected Systems

- IBM Integration Designer 8.5.7, 19.0.0.0, 20.0.0.1, and 20.0.0.2.
- IBM's Business Automation Workflow and Business Process Manager software suites.
- IBM Planning Analytics 2.0 Local and Cloud.
- IBM Kenexa LMS on-premise LMS 6.1 and below.

Vulnerability Overview

These patches coincide with the five vulnerabilities listed below:

CVE-2020-14782 - A bug that could allow attackers to compromise Java SE
CVE-2020-27221 - A stack-based buffer overflow related to Eclipse Open J9 that remote attackers can execute arbitrary code or cause a crash.
CVE-2020-8201 - A Node .js HTTP request smuggling issue.
CVE-2020-8251 - A Node js. Denial of service flaw.
CVE-2020-8252 - A Node .js buffer overflow bug that attackers can exploit to execute arbitrary code.

The first patch addresses security flaws in the IBM Runtime Environment Java 7 and 8. The second one focuses on the IBM Planning Analytics Workspace, a part of Planning Analytics, IBM's collaboration, and management planning software.

Recommendation

Please visit the links in the Patch URL for the appropriate patch. Otherwise, no other mitigations were noted.

Patch URL

http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FWebSphere%2FIBM+Integration+Designer&fixids=8.5.7.0-WS-IID-IFJR63297&source=SAR
http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FWebSphere%2FIBM+Integration+Designer&fixids=19.0.0.2-WS-IID-IFJR63297&source=SAR
http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FWebSphere%2FIBM+Integration+Designer&fixids=20.0.0.1-WS-IID-IFJR63297&source=SAR
http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FWebSphere%2FIBM+Integration+Designer&fixids=20.0.0.2-WS-IID-IFJR63297&source=SAR
https://www.ibm.com/support/pages/node/6406298

Reference

https://www.zdnet.com/article/ibm-patches-vulnerabilities-in-java-runtime-planning-analytics-kenexa-lms/

CRITICAL RCE FLAWS AFFECT VMWARE ESXI AND VSPHERE CLIENT

A VMware vulnerability ESXi and vSphere Client virtual infrastructure have recently been found. This vulnerability could allow attackers to take control of affected systems by executing arbitrary commands. This could give the attacker unrestricted access to the operating system that hosts the vCenter server. This vulnerability has been given a 9.8 out of 10 on the CVSS score, making it a critical severity.

Affected Systems

- 7.0 before 7.0 U1c
- 6.7 before 6.7 U3l
- 6.5 before 6.5 U3n

Vulnerability Overview

A vulnerability, CVE-2021-21972, has been detected within the VMware ESXi and vSphere Client deemed critical. If an attacker can exploit it, this vulnerability would be able to gain access to the server. With this access, the attacker would move through the network gaining access to all the vulnerable data stored, such as the virtual machine information and the different user's information.

CVE-2021-21973 was detected but has a slightly lower score, rating a 5.3. This is not as critical but is still a severe vulnerability. Unauthorized users would be able to access the system giving them the ability to scan the internal network and receive information on its internal network and the open ports.

Recommendation

There is a good possibility that this exploitation can be removed by following the steps in the link below. This is only a temporary workaround until further updates/patches can be completed and deployed later.

Patch URL

https://kb.vmware.com/s/article/82374

Reference

https://thehackernews.com/2021/02/critical-rce-flaw-affects-vmware.html

10,000 MICROSOFT EMAIL USERS CAUGHT IN FEDEX PHISHING ATTACK

Recently, many people have turned to online purchasing for goods and services. Because of this, shipping is at an all-time high. Cybercriminals have taken advantage of this by putting more and more phishing emails into play. FedEx and DHL have played a large part in those deliveries. Now, they appear to be the subject of a recent attack in which as many as 10,000 Microsoft email users have been targeted.

Affected Systems

- Microsoft Email Accounts

Vulnerability Overview

Attackers are sending out emails pretending to be from FedEx and even DHL, targeting Microsoft email users. The attacker's goal is to get these users to enter their work account credentials into their phishing pages.

These emails will start "You have a new FedEx sent to you" and will usually have the date attached to it. When the person opens the email, they will see a link to click on to let them "view" the document. This document that the victim is viewing is usually hosted on a free site such as Box and Quip. This document will look like an honest letter from FedEx, but upon closer inspection, you will be able to locate its origin if it were to come from a free document service such as quip.

In this letter, there will be a link for the person to click on to take them to a page to "see the shipment" information. This page is where the attackers are looking to gain login information. You will enter your information into this fake login screen, and it will be wrong. Many will try different passwords thinking that they are using the wrong one. The phisher is recording all these attempts and has now gained not only your user information but all the different passwords that you may have had or do have for the various work accounts.

Recommendation

First, keep your system security software updated so that it can continue to deal with the growing number of threats. Using multifactor authentication is a great way to keep your systems safe if someone were to get a hold of your password and username.

Reference

https://threatpost.com/microsoft-fedex-phishing-attack/164143/

CLOUD MISHAPS EXPOSED HUNDREDS OF ENTERPRISE PASSWORDS

On February 21st, a notice was released that popular cloud platform ServiceNow had been vulnerable to password access via a stored (but unencrypted) JavaScript file present on all ServiceNow instances. Thus far, more than 600 confirmed enterprises/Universities/government agencies have been known to have been exposed. Attackers who were able to gain administrative privileges through these locations could control any internal employee data, documentation, IT & HR tickets, and other sensitive information.

Affected Systems

- ServiceNow Cloud Platform before version 'Paris'

Vulnerability Overview

In addition to the open JavaScript files mentioned above, the base-64 encoded passwords were not even encrypted at the time. Users of the cloud service have only unknowingly increased their risks by utilizing admin passwords during Simple Object Access Protocols (SOAP), overlooking the provided documentation using unprivileged accounts. Researchers also stated that the vulnerability was as simple as a crafted GET request directed at the credential list, determining what was exposed. Lastly, the incorporated 'Help Desk' feature has been found to have endpoints publicly viewable (these contain passwords), making the entire environment directly compromisable.

Recommendation

Since the software has released a relevant patch since October 8th, it is greatly encouraged that those potentially affected proceed to download this most recent update. Additionally, ServiceNow claims that they are implementing a program to catch/patch any bugs before being exploited.

Patch URL

https://docs.servicenow.com/bundle/paris-release-notes/page/release-notes/available-versions.html

Reference

https://portswigger.net/daily-swig/servicenow-admin-credentials-among-hundreds-of-passwords-exposed-in-cloud-security-blunder?&web_view=true

GOOGLE SHARES POC EXPLOIT FOR WINDOWS 10 GRAPHICS RCE BUG

Google created the Project Zero team that is continually working on hunting bugs in the systems and discovering its vulnerabilities. Google's cybersecurity researchers, Dominik Röttsches and Mateusz Jurczyk, found a critical remote code execution (RCE) bug that impacted Windows graphics. This bug was reported for the first time in November 2020. It was discovered in Microsoft DirectWrite, which is a Windows API for high-quality text rendering.

Affected Systems

- Microsoft

Vulnerability Overview

These attacks usually require interaction with a victim. Bad actors typically host malicious websites containing infected files that will exploit the vulnerabilities of the Microsoft system. Victims were tricked into clicking on a malicious link sent to them through email or instant messaging. This vulnerability allows hackers to execute code to the victim's computer remotely.

Recommendation

Microsoft published a patched version on February 9, 2021. It is recommended to update the software to prevent possible exploitation.

Patch URL

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24093

Reference

https://www.bleepingcomputer.com/news/security/google-shares-poc-exploit-for-critical-windows-10-graphics-rce-bug/

1500 POWERHOUSE VPN SERVERS CAN BE USED TO CREATE DDOS ATTACKS

Recently a security researcher who goes by the name of Phenomite has discovered a flaw in Powerhouse Management VPN Servers. Though it is positive that a researcher has discovered this, it is unfortunate to know that this vulnerability is already known to attackers in the wild. Other sources have observed these exploits and have "clocked" the distributed denial-of-service (DDOS) attacks at 22 Gbps, which is very robust.

Affected Systems

- Powerhouse Management VPN Servers.

Vulnerability Overview

These Powerhouse VPN servers are dangerous because attackers can leverage them to create DDOS campaigns. The main weakness in these servers is an unidentified service that uses port 20811. After conducting a scan last week, Phenomite discovered roughly 1,500 Powerhouse Management VPN Servers that have port 20811 open. This means that there are approximately 1,500 servers that can be used to amplify these potential DDOS attacks.

Recommendation

Block any traffic from Powerhouse Management's IPs and any traffic where the source port is 20811. No patch has been provided as of yet.

Reference

https://www.zdnet.com/article/powerhouse-vpn-products-can-be-abused-for-large-scale-ddos-attacks/

SILVER SPARROW MALWARE INFECTED APPLE MACS

The newly discovered Silver Sparrow malware was recently found to have infected nearly 30,000 Macs. The ultimate goal of this operation remains something of a mystery. The cybersecurity firm Red Canary announced it identified two different versions of the malware. One compiled only for Intel 86_64 and then uploaded to VirusTotal in August 2020. The second was submitted to the database on January 22nd of 2021.

Affected Systems

- macOS

Vulnerability Overview

The newly discovered Silver Sparrow malware was recently found to have infected nearly 30,000 Macs. The ultimate goal of this operation remains something of a mystery. The cybersecurity firm Red Canary announced it identified two different versions of the malware. One compiled only for Intel x86_64 and then uploaded to VirusTotal in August 2020. The second was submitted to the database on January 22nd of 2021. It is compatible with both Intel x86_64 as well as the M1 ARM64 architectures. Adding to the confusion, the x86_64 binary, upon execution, simply states the message "Hello, World!" The M1 binary displays "You did it!" Researchers suspect these messages are being used as a placeholder. Silver Sparrow is the second piece of malware to contain code that runs natively on Apple's new M1 chip. A Safari adware extension named GoSearch22 was discovered recently and ran on the latest Macs powered by the new processors.

Recommendation

If your Apple products are using the new M1 chip, please pay attention to Apple's latest updates related to the Sliver Sparrow malware. Install antivirus and anti-spyware software or implement a firewall, intrusion detection system (IDS), and intrusion prevention system (IPS). Please keep the software updated.

Reference

https://thehackernews.com/2021/02/new-silver-sparrow-malware-infected.html

TWO FACTOR AUTHENTICATION COMPROMISED AFTER PHISHING ATTEMPTS

Software-as-a-Service (SaaS) attacks have been increasing due to the increased reliance upon them for services such as email, user management, sharing, and storage. This increases the surface area available for any potential attacker. On top of that, security teams often have poor visibility of the interactions within these siloed platforms.

This is where two-factor authentication (2FA), or multifactor authentication (MFA), is usually depended upon to help secure these resources through the need for additional metrics such as SMS or Email codes, biometrics, or personal knowledge. However, there are ways for attackers to bypass these extra measures subtly.

Affected Systems

- All users that click on malicious phishing links and fall victim to social engineering attempts

Vulnerability Overview

Attacks that have been observed in the wild have started with employees of an organization clicking on a malicious link from a phishing email. This is followed by unusual log-on locations with successful 2FAs, manipulated user details, and registered telephone numbers.

There are a few ways to compromise 2FA, such as implementing SIM swapping or using a malicious OAuth app, or use real-time social engineering to extract needed passcodes from victims. From here, attackers usually set up new email rules, searching for sensitive data, observing writing styles, and deleting emails that may alert the user to compromise.

Recommendation

Examine emails thoroughly before opening attachments or clicking on links, confirm registered phone numbers, do not give potentially sensitive information to unsolicited callers, and review your email settings every so often for any malicious changes.

Reference

https://www.darktrace.com/en/blog/two-factor-authentication-2-fa-compromised-microsoft-account-takeover/

PROTECT YOUR BUSINESS EMAIL SECURITY BY EMAIL AUTHENTICATION

Business Email Compromise (BEC) is an attacker's favorite tool for attacking governmental, commercial, and non-profit organizations. It quickly leads to data and security breaches ending in losing reputation and financial assets for the companies.

Affected Systems

- Email Systems

Vulnerability Overview

Attackers utilize sophisticated social engineering techniques, including phishing and email spoofing. Impersonation using the authoritarian positions as a CFO or CEO makes these attacks more successful and lucrative. Some adversaries like the Russian cybergang Cosmic Lynx are known to carry out phishing attacks with perfect wording. BEC has impacted more than 70% of the institutions worldwide and results in the loss of billions of dollars annually. Email authentication techniques like DMARC provide verifiable data about the sender's address, and it is one of the best solutions for protecting our email security against impersonation attacks.

Recommendation

Steps to Protect against BEC include:

- Implement DMARC for your domain.

- Identify the official email sources of your domain.
- Publish SPF-DKIM and DMARC records in your DNS for your domain.
- Configure Enforcement on DMARC Policy.
- Beginning with monitoring the only option and eventually shifting to higher levels of enforcement is recommended.
- Establish an effective monitoring and reporting system.
- Always stay under the 10 DNS Lookup Limit.
- Ensure TLS Encryption of Emails in Transit (Protection against MITM attacks).
- Enable SMTP TLS Diagnostic Reporting on Issues in Email Delivery

Reference

https://thehackernews.com/2021/02/how-to-fight-business-email-compromise.html

MALFORMED URL PREFIX PHISHING ATTACKS

There has been a nearly 6000% jump in attacks using "malformed URL prefixes." These attacks evade protections and send phishing emails that appear legitimate unless you look closely at the prefix symbols before the URL. Researchers from GreatHorn were the first to report these attacks.

Affected Systems

- All Systems

Vulnerability Overview

There has been a massive uptick in malformed URL prefix phishing attacks as of late. GreatHorn has reported a nearly 6000% spike in these types of attacks. The URLs are malformed and do not utilize the standard protocols such as HTTP:// or HTTPS://. Instead, they use HTTP:/\ in their URL prefix. GreatHorn explains that the address's slashes are primarily superfluous, so browsers and many scanners do not look at them. The URLs are not categorized as "bad" profiles, so simple email scanning programs cannot detect them. They can also slip past the human eyes that are not used to looking in the prefix for indicators of suspicious activity.

Recommendation

Please be aware of suspicious URLs that are not facing the standard direction (the dashes should appear as HTTP:// or HTTPS:// instead of http:/\, for example). This is an indicator of suspicious activity.

Reference

https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/

FLORIDA CITY WATER SUPPLY HACKED

On February 5th, the water controller discovered the remote compromise system at the City Water of Oldsmar. An unknown bad actor has remotely gained access to the plant water system and intentionally alter the level of sodium hydroxide from 100 parts per million to 11,100 parts per million. Sodium hydroxide is used to control acidity in consumable water. It can cause skin irritation and be harmful to people when bad actors maliciously control it.

Affected Systems

- City Water of Oldsmar

Vulnerability Overview

The details of the remote compromise are minimal. The water controller who was there during the compromise was able to change the level of sodium hydroxide back to its original number before it took effect. The hacker was using a remote access software called TeamViewer to access the City Water computer system. The remote hacker used less than 5 minutes to compromise the system and changed the sodium hydroxide level. For this incident, the human-machine interface (HM) is targeted.

Recommendation

Basic security awareness training is recommended. Organizations should provide security best-practices by controlling non-authorized access to the system (2-step verification and setting up a passcode to unlock the software). Password policies should be put in place. Ensure systems and software are patched.

Reference

https://www.securityweek.com/remote-hacker-caught-poisoning-florida-city-water-supply

PYTHON BUFFER OVERFLOW VULNERABILITY

Python is a popular programming language that has been around for many years and is a high-level, general-purpose language. Many developers use it for various applications such as web applications and security application use, and some popular programs written in Python are Instagram, Spotify, and Dropbox.

Affected Systems

- Python versions before 3.9.2 and 3.8.8

Vulnerability Overview

The vulnerability listed affects python versions earlier than 3.9.2 and 3.8.8. The vulnerability that is being disclosed is a buffer overflow that could lead to remote code execution, which means that a threat actor can make unauthorized changes.

The vulnerability is associated with PyCArg_repr in _ctypes/callproc.c and affects applications using floating-point numbers that are not verified as input.
Sprintf is the cause of this because it is used unsafely, and Sprintf is a function used to format strings.

Recommendation

Update to the latest version of Python.

Patch URL

https://www.zdnet.com/article/python-programming-language-hurries-out-update-to-tackle-remote-code-vulnerability/?&web_view=true

Reference

https://www.zdnet.com/article/python-programming-language-hurries-out-update-to-tackle-remote-code-vulnerability/?&web_view=true

JAVASCRIPT PACKAGE MANAGER PATCHED FOR COMMAND INJECTION VULNERABILITIES

The systeminformation library used for a popular package manager, Node.js (850K downloads), was recently patched to cover vulnerabilities susceptible to command injection attacks. The problem stems from developers using the systeminformation library in ways that the maintenance team did not anticipate.

Affected Systems

- Applications using NPM's system information package versions < 5.3.1

Vulnerability Overview

The systeminformation package was meant to be a back-end exclusive package, but developers have been seen giving users access to certain package functions. This user access opens these applications to possible command injections because systeminformation functions did not provide sufficient parameter checks.

The four functions that were found to be vulnerable to command injections were:

- si.inetLatency()
- si.inetChecksite()
- si.services()
- si.processLoad()

Recommendation

Review package documentation for functions where manual sanitation needs to be implemented.

Reference

https://portswigger.net/daily-swig/popular-node-js-package-vulnerable-to-command-injection-attacks

SECURITY BREACHES ON CLUBHOUSE SOCIAL MEDIA

Clubhouse, a new addition to voice-based social media, is now turning one year old. This application is only available for invitation-only IOS users, and over 8 million users have already installed this application on their phones. Over the past weekend, Clubhouse has raised its security concern and banned users who have breached Clubhouse room audio feeds and steam them on other websites.

Affected Systems

- Clubhouse

Vulnerability Overview

On February 13th, 2021, Stanford Internet Observatory (SIO) warned consumers about the chats breached. Since Clubhouse is a real-time audio-based chat room, users should be aware that all their chat conversations are being recorded. Clubhouse has confirmed that all their web traffics are being routed to Agora's server based in China and Silicon Valley. The People's Republic of China could ask for audio investigation required cybersecurity laws. This could lead consumers to reveal their information to data collection.

Recommendation

The malicious code designed to breach Clubhouse has been blocked. Updating to the latest version of Clubhouse would be the best security practice consumers could do at the time.

Reference

https://threatpost.com/clubhouse-conversations-recorded/164158/

TDOS ATTACKS EMERGENCY FIRST-RESPONDER SERVICES

A telephone Denial of Service (TDoS) attack is a DoS attack on a telephone system. TDoS attacks are on the rise, attacking critical First-Responder Services (Police, Fire, Ambulance Services). The attack is designed to flood a telephone system's bandwidth with junk calls and stops incoming and outgoing calls.

Affected Systems

- Citizens, Police, Fire, and Ambulance services.

Vulnerability Overview

TDoS attacks were first discovered in July 2012. A TDoS attack aims to make sure junk calls stay active for a long time to flood the target's telephone resources and cause a delay and prevent legitimate incoming calls. TDoS has been targeting Public Safety Answering Points (PSAPs), which primarily oversee transferring calls to emergency services. According to the FBI, the attack comes in the form of manual or automated incoming calls. TDoS attacks usually started from using different social networks, encouraging people to flood certain telephone numbers with calling campaigns.

Automated TDoS calls use VoIP and session initiation protocol (SIP) to make hundreds of calls at a time. The TDoS attack is cheap and mainly used by hacktivists. Malicious actors also use this type of attack to target private companies by mimicking the collection agency to collect fees. Bad actors will also use this attack to harass people for fun.

Recommendation

Alternative ways to reach emergency services when 911 is unavailable include:

- See if text-to-911 is available in your area.
- Contact local emergency services authorities.
- Be prepared to use a non-emergency contact number for all services you need.
- Sign up for automated emergency notifications.
- Follow social media for local emergency news.

Reference

https://threatpost.com/tdos-attacks-emergency-first-responder/164176/

FIREFOX INTRODUCES TOTAL COOKIE PROTECTION, BUG FIXES

Mozilla Firefox 86 will introduce a novel feature that may have interesting impacts on browsing with Total Cookie Protection. Further, some bugs were fixed in the latest release. Given the possible implications, this may be something for administrators to watch.

Affected Systems

- Firefox

Vulnerability Overview

With the release of Firefox 86, the Mozilla Foundation introduced the concept of Total Cookie Protection. In short, the organization is making a push against tracking cookies by having each tab put into its own "cookie jar." With limited exceptions made for cross-site cookies used for non-tracking functions, such as for federated sign-ins. This works in conjunction with previously released versions that aim to block hidden trackers and other protections.

In sum, each website visited will have its own cookies, caches, and even network connections isolated. Doing this works to prevent supercookies, which cannot be deleted when clearing cache, from tracking browsing activity via cookies.

The update includes stability and performance enhancements made to WebGL and canvas and some bug resolutions, though no issues were of a critical nature.

Recommendation

With any patch or upgrade, we recommend testing before any deployment. If your organization employs supercookies or other tracking cookies, please verify this activity is necessary or can be worked around before deployment.

Reference

https://www.bleepingcomputer.com/news/software/firefox-86-gets-a-privacy-boost-with-total-cookie-protection/

CRITICAL CISCO VULNERABILITY ALLOWS ATTACKERS TO BYPASS AUTHENTICATION

Cisco's newest vulnerabilities make it possible for remote, unauthenticated attackers to gain privileged access to hardware and software. These vulnerabilities stem from faulty token validation, faulty administration of internal management services, and a lack of access control for network data services.

Affected Systems

- ACI Multi-Site Orchestrator Version 3.0 running on Cisco's Application Service Engine.
- Cisco Nexus Switches Series 3000 and 9000.
- Cisco’s Application Service Engine Software 1.1 and earlier.

Vulnerability Overview

CVE-2021-1338 is considered a critical vulnerability (10 out of 10 CVSS score) because it could allow an attacker to successfully remote into Cisco's ACI MSO software through a malicious API request. This vulnerability stems from faulty token validation on the ACI MSO API endpoint.

CVE-2021-1361 (9.8 out of 10 CVSS score) could allow a remote attacker to bypass authentication to manipulate, create and delete files using root privilege on Cisco Nexus switches. This vulnerability stems from the faulty administration of internal management services causing TCP port 9075 to listen and respond to external requests.

CVE-2021-1393 (9.8 out of 10 CVSS score) could allow remote, unauthenticated attackers to view device information, make configuration changes and create diagnostic files through privileged access of host-level operations. This vulnerability stems from lacking access controls for services involving Cisco's Application Service Engine Software's network data.

Recommendation

Keep the newest updates and patches applied for the above software and hardware.

Patch URL

https://tools.cisco.com/security/center/publicationListing.x

Reference

https://threatpost.com/cisco-critical-security-flaw/164255/