BRAINTRACE

THREAT ADVISORY REPORT

MARCH 25, 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.

CISA RELEASES NEW SOLARWINDS MALICIOUS ACTIVITY DETECTION TOOL

CISA (Cybersecurity and Infrastructure Security Agency) has released a new tool in the fight to detect post-compromise malicious activities dealing with the SolarWinds hackers within enterprise environments. The new tool officially named CHIRP comes on the heels of its predecessor Sparrow. CHIRP looks for compromise within on-premises environments, while Sparrow scans for signs of compromise within M365 or Azure environments only.

Affected Systems

- Windows environments using SolarWinds

Vulnerability Overview

CHIRP is designed to search for different indicators of compromise (IOCs) associated with the malicious activity specified in CISA alerts AA20-352A and AA21-008A, which could have rolled into an on-premises environment. The alerts mentioned above refer to government agencies, critical infrastructure, and private organizations using the compromised SolarWinds Orion products, including Microsoft 365 and Azure environments as access vectors.

CHIRP is a command-line executable with a dynamic plugin and indicator system which will search for different signs of compromise. It will use various plugins to search the event logs and registry keys while running YARA rules scanning for signs of APT tactics and techniques. CHIRP also has an internal file that contains the list of IOCs that CISA has associated with the malware and APT activity.

Recommendation

CISA has advised that organizations use CHIRP to examine Windows event logs for artifacts associated with this activity. It has also been suggested that it be run to examine the Windows registry for evidence of intrusion and query Windows network artifacts. CISA has also advised that CHIRP be used to apply YARA rules to detect malware, backdoors, or implants.

Patch URL

https://github.com/cisagov/Sparrow

Reference

https://www.bleepingcomputer.com/news/security/cisa-releases-new-solarwinds-malicious-activity-detection-tool/

CYBERATTACK METHODS AND TACTICS CHANGES AFTER COVID-19

A year after the COVID-19 pandemic, cybercriminals have changed their methods and tactics due to how people have changed the way they work and living lifestyles. Attackers on the internet actively exploit phishing scams with COVID-19 themes and brute-Force attacks on remote users using Remote Desktop Protocol (RDP).

Affected Systems

- Remote workers

Vulnerability Overview

According to Kaspersky, phishing emails ranked the most effective type of attack during the COVID-19 pandemic. Those emails are campaigning for N95 masks and hand sanitizer, which ask the victims to put in their payment information. Cybercriminals impersonate leading authorities, such as the CDC and the World Health Organization, by tricking targeted users and giving them what they considered are essential updates from leaders when those updates were malware.

Attackers also send phishing emails regarding "delayed shipments" because online shopping has become the only way for many to shop during the 2020 lockdowns. Shipping services ranked the ten most spoofed companies for phishing email attacks. Cybercriminals would claim in the email that due to COVID, the victims' delivery shipment would be delayed and asking them to verify the delivery address. This is an easy giveaway due to the ongoing pandemic when the target users are unaware and click on the attachment with trojan and backdoor attach to it.

During the 2020 pandemic, according to the analysis, millions of people were assigned to work remotely from home. Remote employees become the target for remoting into corporate resources using their personal computers on an unsecured network vulnerable to brute force attacks. Remote Desktop Protocol (RDP) connections are on the rise, and it is the most popular remote protocol used by organizations. It surged from 93.1 million connections in February to 277.4 million connections worldwide in March.

Recommendation

To protect yourself from phishing emails, it is recommended to have email scanning and spam filters to help filter out spam and phishing emails. Also, be very cautious when opening email attachments.

Reference

https://threatpost.com/cyberattacks-fundamental-changes-covid-19/164775/

NEW ZOOM SCREEN-SHARING BUG LETS OTHER USERS ACCESS RESTRICTED APPS

There is a new unpatched security vulnerability in the popular meeting app ZOOM. A user-friendly functionality within ZOOM is the screen sharing feature. The screen sharing feature allows the user to

share their desktop or even a portion of the screen. This recent vulnerability within the screen sharing feature can accidentally enable sensitive information to be leaked.

Affected Systems

- ZOOM versions 5.4.3 and 5.5.4 on both Windows and Linux systems.

Vulnerability Overview

The flaw currently filed as CVE-2021-28133 comes from a screen sharing function glitch within the highly popular meeting app ZOOM. The vulnerability is only a medium severity at this time, for the attacker would have to be a participant in the meeting. However, the information shared within that meeting can include damaging or highly classified information and, if leaked, could have more than a medium severity result on the company or presenter. While the information that would be shared would only be shown briefly, there are possibilities that someone can be recording the meeting itself. When the meeting is over, the attendee would be able to review the screen share and catch the moment of the information leak.

This vulnerability has been brought to ZOOM, and they have stated that there is an upcoming release scheduled to go live on March 22nd, and it will address this flaw.

Recommendation

It is recommended that users who use the screen sharing functionality follow a "Clean Virtual Desktop" policy until a patch is issued. There is a scheduled update on March 22nd that will address this flaw.

Reference

https://thehackernews.com/2021/03/new-zoom-screen-sharing-bug-lets-other.html

PHISHING WEBSITES DETECT VIRTUAL MACHINES TO EVADE DETECTION

Threat actors behind phishing websites are now using JavaScript to detect virtual machines to bypass detection. The JavaScript is used to determine whether a user is visiting from within a headless device or Virtual Machine. Cybersecurity researchers commonly use Virtual Machines or headless devices to check if a website is a phishing site.

Affected Systems

- All Systems

Vulnerability Overview

The phishing kit checks to see if the browser is using a software renderer and the height and width of the user's screen to evade detection. Software renderers such as SwiftShader, LLVMpipe, or VirtualBox indicate that the browser is running on a Virtual Machine(VM) or an unattached monitor. The script will also check whether the user's screen height or width is less than 100 pixels or if the screen has a color

depth of less than 24-bits. If any of the indicators listed are deemed true, then a message will appear in the browser's developer console, and the script will show a black page instead of the phishing landing page.

Recommendation

It is recommended to be aware of phishing scams and sites and to have strong security practices.

Reference

https://www.bleepingcomputer.com/news/security/phishing-sites-now-detect-virtual-machines-to-bypass-detection/

FBI WARNS OF PYSA RANSOMWARE ATTACKS

The Federal Bureau of Investigation's (FBI) Cyber Division has warned the Pysa ransomware. There have been Pysa ransomware attacks targeting private companies, education institutions, government, and healthcare sectors since October of 2019. In the past year, there has been an increase in attacks from ransomware. Pysa, also known as Mespinoza, is used to encrypt files on user's devices and servers.

Affected Systems

- All systems

Vulnerability Overview

The threat actors behind Pysa gain access to the user's network via a malicious attachment from a phishing email or compromised Remote Desktop Protocol credentials. Once the threat actors gain access, it begins the process of encrypting all connecting devices and data, including tax information and personally identifiable information (PII), to extort money from the victim. The ransomware also adds the file extension, [.]pysa, to every encrypted file. It also deactivates any antivirus software to evade detection. The ransomware also creates a ransom note with instructions on contacting the threat actors through email and paying the ransom. The ransom note is displayed on the login screen of the infected device.

Recommendation

The FBI has a list of recommended mitigations, including backing up data offline regularly, install updates as soon as they are available, and implement network segmentation. For the complete list of recommendations, please see the Reference article.

Reference

https://www.bleepingcomputer.com/news/security/fbi-warns-of-escalating-pysa-ransomware-attacks-on-education-orgs/

CISCO SMALL BUSINESS ROUTES LATEST PATCH

This past week, Cisco has released a new advisory related to several small business routers. This vulnerability could be exploited remotely with an authenticated attacker. A successful attack could lead to remote code execution and DoS. This vulnerability has been given a score of 7.2 on the CVSS scale.

Affected Systems

- RV132W ADSL2+ Wireless-N VPN Router < v1.0.1.15
- RV134W VDSL2 Wireless-AC VPN Router < v1.0.1.21

Vulnerability Overview

This vulnerability exists in the router's web management interface and its ability to properly validate user input. An attacker can successfully exploit this vulnerability through a specially crafted HTTP request to execute code as a root user.

Recommendation

Upgrade to the latest software.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p

COPPERSTEALER MALWARE TARGETS ADVERTISING AND BUSINESS ACCOUNTS

A newly discovered malware called CopperStealer has been observed stealing credentials to advertising and business accounts of platforms such as Facebook, Google, Amazon, Apple, Bing, Paypal, Tumblr, and Twitter.

CopperStealer is a password and cookie thief capable of downloading data and unloading additional malware after initial malicious activity. CopperStealer has been likened to other pieces of malware such as SilentFade, StressPaint, FacebookRobot, and Scranos.

Affected Systems

- Devices that have visited websites promising free license keys to software

Vulnerability Overview

CopperStealer has been observed coming from sites that promise key generation services for legitimate software licenses. In the first 24 hours of Cloudflare activating a sinkhole for two malicious domains, 69,992 HTTP requests were recorded from 5,064 different IP addresses in 159 countries, which resulted in 4,655 infections.

Known websites transmitting CopperStealer among other pieces of malware:

- keygenninjs[.]com
- piratewares[.]com
- startcrack[.]com
- crackheap[.]net

CopperStealer downloads configurations from C2 servers to retrieve a file named 'xldl.dat,' which poses as a legitimate download for Xunlei by Xunlei Networking Technologies. An exposed API in the Xunlei application retrieves the configurations needed for a follow-up binary.

Recommendation

Do not visit unknown websites under the pretense of free products.

Reference

https://threatpost.com/copperstealer-hijacks-accounts/164919/

REVIL RANSOMWARE'S NEW FEATURE CAN OPERATE IN WINDOW'S SAFE MODE

The REvil ransomware, also known as Sodinokibi, is a part of a ransomware-as-a-service (RaaS) operation that works with other malicious parties to distribute the ransomware. In the latest sample found in the wild, a new feature was found called '-smode,' which installs the ransomware through Windows Safe Mode.

Affected Systems

- Windows devices

Vulnerability Overview

REvil's new feature is a command-line tool '-smode,' which causes a device to enter Safe Mode on the next reboot. The commands involved follow as:

'bootcfg /raw /a /safeboot:network /id 1
bcdedit /set {current} safeboot network'

This is followed by the creation of an autorun file called '*franceisshit', which performs the following command once Safe Mode has been activated (The * allows the autorun file to execute in safe mode):

'bcdedit /deletevalue {current} safeboot'

Once the user logs in, the computer is forced to restart in Safe Mode with Networking after creating another malicious autorun file called 'AstraZeneca,' which contains the REvil ransomware sans the -smode command. After the next login, REvil starts to encrypt files and does not allow applications to be opened. Opening Task Manager with Ctrl+Alt+Delete will enable you to see the executable.

Once encryption is complete, the remaining boot sequence occurs, and a ransom note is available.

Recommendation

Use caution when opening email attachments and visiting websites.

Reference

https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

OPERATION DIÀNXÙN: THE MUSTANG PANDA 5G CAMPAIGN

Researchers with McAfee recently uncovered a campaign believed to be executed by Mustang Panda, an APT group associated with China. The targets have been spread across North America, Europe, and Southeast Asia, with telecommunications organizations being the campaign's primary organizational targets.

Affected Systems

- Telecom and Wireless providers

Vulnerability Overview

Dubbed Operation Diànxùn by McAfee, the primary motivation seems to be the recent bans on Chinese equipment in 5G rollouts worldwide. The group, Mustang Panda, is said to have a history of working at the Chinese government's behest.

In the campaign, targeted users are linked to a web page made to look like a Huawei career opportunities page. Users will download malware from this website that masquerades as Adobe Flash Player, which also looks like a legitimate site to download the regular product.

The software in question establishes persistence and backdoor on the affected system. A secondary DotNet malware is installed, which includes a tool to manage backdoors.

Indicators of Compromise

SHA256 hashes

422e3b16e431daa07bae951eed08429a0c4ccf8e37746c733be512f1a5a160a3
8489ee84e810b5ed337f8496330e69d6840e7c8e228b245f6e28ac6905c19f4a
c0331d4dee56ef0a8bb8e3d31bdfd3381bafc6ee80b85b338cee4001f7fb3d8c

89a1f947b96b39bfd1fffd8d0d670dddd2c4d96f9fdae96f435f2363a483c0e1
b3fd750484fca838813e814db7d6491fea36abe889787fb7cf3fb29d9d9f5429
9ccb4ed133be5c9c554027347ad8b722f0b4c3f14bfd947edfe75a015bf085e5
4e7fc846be8932a9df07f6c5c9cbbd1721620a85c6363f51fa52d8feac68ff47
0f2e16690fb2ef2b5b4c58b343314fc32603364a312a6b230ab7b4b963160382
db36ad77875bbf622d96ae8086f44924c37034dd95e9eb6d6369cc6accd2a40d
8bd55ecb27b94b10cb9b36ab40c7ea954cf602761202546f9b9e163de1dde8eb
7de56f65ee98a8cd305faefcac66d918565f596405020178aee47a3bd9abd63c
9d4b4c39106f8e2fd036e798fc67bbd7b98284121724c0f845bca0a6d2ae3999
ac88a65345b247ea3d0cfb4d2fb1e97afd88460463a4fc5ac25d3569aea42597
37643f752302a8a3d6bb6cc31f67b8107e6bbbb0e1a725b7cebed2b79812941f
d0dd9c624bb2b33de96c29b0ccb5aa5b43ce83a54e2842f1643247811487f8d9
260ebbf392498d00d767a5c5ba695e1a124057c1c01fff2ae76db7853fe4255b
e784e95fb5b0188f0c7c82add9a3c89c5bc379eaf356a4d3876d9493a986e343
a95909413a9a72f69d3c102448d37a17659e46630999b25e7f213ec761db9e81
b7f36159aec7f3512e00bfa8aa189cbb97f9cc4752a635bc272c7a5ac1710e0b
4332f0740b3b6c7f9b438ef3caa995a40ce53b3348033b381b4ff11b4cae23bd

More information can be found here: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-operation-dianxun/

Recommendation

Given the nature of the campaign, we would recommend training and education regarding social engineering campaigns. Specifically, paying attention to URLs and other phishing indicators usually stops such campaign attempts before they get started.

Reference

https://www.darkreading.com/threat-intelligence/chinese-apt-targets-telcos-in-5g-related-cyber-espionage-campaign/d/d-id/1340427

GOOGLE RELEASED POC FOR SPECTRE ATTACK

The Spectre attack was first discovered back in 2019. It is a vulnerability of a computer processor that can be exploited and can cause permanent physical damage to the affected host system. Google has recently published a proof-of-concept (POC) exploit to simulate Spectre attacks against the Chrome browser that leaks data from different websites.

Affected Systems

- Modern processors (Intel and AMD)
- Android, ChromeOS, Linux, macOS, and Windows Operating Systems.

Vulnerability Overview

Google information security engineers Stephen Röttger and Artur Janc shared a PoC exploiting a Spectre attack against the Chrome browser. However, the issues are not specific to Chrome. Researchers also expect other browsers to be vulnerable to this exploitation vector.

The POC JavaScript code works on Chrome 88 on an Intel Skylake CPU, allowing data extraction from memory at a speed of 1KB/s. Google researchers also believed the PoC would also work on other types of CPUs.

The Spectre attack uses speculative execution techniques in today's CPUs to enhance performance in swiping sensitive data.

The demonstration of the Spectre attack is available at the URL below:

https://leaky.page/

Recommendation

To protect your system from a Spectre attack, it is recommended for developers to use a hardening technique called kernel page table isolation (KPTI) and a new security mechanism to prevent hardware attacks.

Standard protection options to consider include:
X-Content-Type-Options
X-Frame-Options headers
the use of Same Site cookies

Reference

https://threatpost.com/google-spectre-poc-exploit-chrome/164787/

MICROSOFT HALTS ROLLOUT OF WINDOWS 10 KB5001649 EMERGENCY UPDATE

Microsoft has decided to pause the rollout of the Windows 10 KB5001649 update. There have been multiple reports of installation issues as well as reported crashes within this update. In response, Microsoft decided to release an emergency update of previously released KB5001567.

Affected Systems

- This update affects Microsoft 10 operating system users.

Vulnerability Overview

The recent Microsoft update KB5001649 has been paused due to reported crashes and multiple installation issues. Many of the users had been experiencing "APC_INDEX_MISMATCH for

win32kfull.sys" which causes crashes when printing. Because of these issues, Microsoft issued a new out-of-band update (KB5001567) to replace it. This update is said to fix the printing errors, and once the older update is replaced, the printing errors will stop.

Recommendation

Microsoft has released this update KB5001649 thru Windows Update as an optional update replacing the KB5001567. Updating to the newer patch is recommended.

Reference

https://www.bleepingcomputer.com/news/microsoft/microsoft-halts-rollout-of-windows-10-kb5001649-emergency-update/

METAMORFO BANKING TROJAN

Metamorfo, also known as Mekotio, first emerged in April 2018 as a banking trojan targeting clients in Latin American and European countries. In February 2020, a newly developed Metamorfo discovered misusing AutoHotkey (AHK) and the AHK compiler to avoid the detection and swipe users' personal information. AHK is a Windows scripting language developed for keyboard hotkeys creation.

Affected Systems

- Banks in Latin American and European countries

Vulnerability Overview

The Metamorfo trojan uses two emails as the first infector vector. One is an intended request to have the users download a password-protected file, and the second email is a pending forgery legal documents with a link to download. ZIP file. Both files have a .ZIP file that will be downloaded to the target machines. This .ZIP file has three files: the actual AutoHotkey compiler executable, a malicious AutoHotkey script, and the Metamorfo Banking Trojan. These files will be extracted, renamed, and saved in C:\\ProgramData.

After the files are saved on the target computers, the script will execute the AutoHotkey compiler and import Metamorfo trojan into the compiler's memory. Metamorfo will then run using the compiler and avoid being detected by using the signed binary. The run key will be used to run the execution when the computer reboot by executing the renamed AutoHotkey compiler's copy.

The Metamorfo Trojan enables removing auto-suggest data entry fields in web browsers, not allowing the victims to use their saved password and force them to type it out. Metamorfo uses a keylogger to steals victims' credentials. This trojan is targeting banking pages that are listed as strings in AutoHotkey compiler process memory. When the target victims open a baking page, Metamorfo trojan covers the page with its forgery webpage and steals victims' credentials.

Recommendation

To protect yourself from Metamorfo banking trojan, it is recommended to add multifactor authentication, use a password manager, email scanning and monitoring, and be very cautious when opening email attachments.

Reference

https://threatpost.com/metamorfo-banking-trojan-autohotkey/164735/

MICROSOFT PATCH TUESDAY - MARCH 2021

As surely as the tides will roll in both their highs and lows, as the moon is apt to wax and wane, and as the taxman will come for his due, Microsoft's monthly release of patches for their products, known colloquially as Patch Tuesday, has come to fruition for March. In this month's cycle, Microsoft patch 14 vulnerabilities rated as Critical and two previously known bugs.

Affected Systems

- Microsoft products

Vulnerability Overview

In this month's release, five of the patches cover issues with ProxyLogon. CVE-2021-26855, 2021-26857, CVE-2021-26858, and CVE-2021-27065 are issues that allow an attacker to break into Microsoft's Exchange Servers. As we have covered previously, Microsoft issued an urgent out-of-band patch for these issues, and customers were urgently pressed to patch their servers. Not patching allows for the installation of backdoors which compromise the integrity of the target server. Microsoft took the unusual step of further releasing its update for older versions of Exchange that reached End of Life.

Patches were also issued for CVE-2021-26877 and CVE-2021-26897. These are remote code execution flaws that were covered previously as well. Rating as a near-perfect 9.8 using CVSS 3.0 metrics, urgent patching was advised as well. Hyper-V, SharePoint Server, and Azure Sphere patches were also issued for bugs that were rated as either High or critical.

Recommendation

Even if these issues were offered patches before the Patch Tuesday cycle, we still recommend testing and verifying your patch levels were possible. Microsoft issues a cumulative patch for most of its products monthly. As such, we suggest applying the latest versions of those if possible.

Reference

https://thehackernews.com/2021/03/microsoft-issues-security-patches-for.html

ZEN CART REFLECTED XSS VULNERABILITY

This reflected cross-site scripting (XSS) vulnerability was privately reported to the vendor back in January 2020 by researchers from usd AG, HeroLab. The vulnerability was patched silently and only saw public disclosure, including a POC exploit, on February 26, 2021. This is considered an easy vulnerability to exploit with moderate impact if an attack is successful.

Affected Systems

- Zen Cart version 1.5.6d and below

Vulnerability Overview

Reflected XSS vulnerabilities are not persistent and require interaction by a victim to trigger a payload. In this case, HTML code (including JavaScript) is added as a value to the main_page URL parameter in one of two files (/includes/templates/template_default/common/tpl_main_page.php and /includes/templates/responsive_classic/common/tpl_main_page.php), where it is injected into the web page when a victim clicks on the link.

An attacker can exploit this vulnerability to abuse the trust a victim has in a domain and make them more willing to click on a link that has been sent to them. The malicious JavaScript payload is injected into the victim's browser could download files or send information to the attacker.

Recommendation

Apply vendor patches after appropriate testing.

Patch URL

https://www.zen-cart.com/

Reference

https://herolab.usd.de/security-advisories/usd-2019-0069/

VULNERABLE DUCKDUCKGO BROWSER EXTENSION

Privacy is an essential topic for cybersecurity, whether using protocols that encrypt data during data transmission or even using a VPN tunnel when using open WIFI networks to prevent an unauthorized user from sniffing the traffic. DuckDuckGo provides a service within a browser extension that would allow a user to search for various things without being tracked by third-party software. According to this article, the vulnerability was discovered in the DuckDuckGo privacy essentials.

Affected Systems

- Internet Browsers (Chrome, Firefox, Edge)

Vulnerability Overview

The vulnerability discovered is Universal Cross-Site Scripting (UXSS) which exploits browser extensions and can allow attackers to see everything, even a user's private banking information. Attackers could also change visited web pages and customize them to their liking.

So far, there is an update for Chrome and Firefox browsers, but nothing yet for Edge browsers. To run this exploit successfully, the attacker would need control of the http://staticcdn.duckduckgo.com, and therefore, the attacker needs control of the server.

Recommendation

Update browsers to the latest versions and avoid using the Edge browser until an update can be provided for this browser.

Reference

https://portswigger.net/daily-swig/duckduckgo-browser-extension-vulnerability-leaves-edge-users-open-to-potential-cyber-snooping?&web_view=true

NEW BOTNET TARGETS NETWORK SECURITY DEVICES

Cybersecurity researchers from Palo Alto Networks' Unit 42 published details of an attack from a new botnet. They published research on February 16, 2021. These attacks are executed by the new botnet, which is exploiting connected devices. Researchers started tracking down botnet activity and have noticed that it took more than a month for the operator to implement exploits. These vulnerabilities were detected in the SSD Secure Disclosure program. These vulnerabilities are still being exploited in the wild.

Affected Systems

- All systems

Vulnerability Overview

After hackers compromised the victim's device, they would drop binaries to complete malicious actions like brute-force attacks. Devices will be infected with some type of Mirai botnet malware. This malware is turning victim's computers into bots that will be used in botnet network attacks. Researchers wrote that user-provided data had not been filtered, which allowed attackers to complete arbitrary commands with escalated privileges. Binaries that were used in these attacks are:

lolol.sh
install.sh
nbrute.[arch]
combo.txt
dark.[arch]

Indicators of Compromise

URLs:

203[.]159.80.241/bins/dark.arm5
203[.]159.80.241/bins/dark.arm6
203[.]159.80.241/bins/dark.arm7
203[.]159.80.241/bins/dark.m68k
203[.]159.80.241/bins/dark.mips
203[.]159.80.241/bins/dark.mpsl
203[.]159.80.241/bins/dark.ppc
203[.]159.80.241/bins/dark.sh4
203[.]159.80.241/bins/dark.x86
203[.]159.80.241/bins/dark.arm7
203[.]159.80.241/bins/dark.arm6
203[.]159.80.241/bins/dark.arm5
203[.]159.80.241/bins/dark.mpsl
203[.]159.80.241/bins/dark.mips
203[.]159.80.241/bins/dark.x86
203[.]159.80.241/bins/dark.ppc
203[.]159.80.241/bins/dark.m68k
45[.]133.1.133/bins/dark.ppc
45[.]133.1.133/bins/dark.m68k

SHA 256:

60135a7817a0a1734c2e211a8613873548f4611fddc8666890f6a69860c43e61
087fc3206ddb94e80118e7e7f0215c88409a0071b657d21071e15b7917f7cc4e
33f75999a3b4c354b6281399e541b97fd6463c5cd2ab13a538522d72a8870f30
02d48570f1089e2e7f4f9256bb033136c773834af31054e477e094e48cba110e
45ff08b1de872379f965d423a0f4e1f2e82f0ea8d101220b83d3aed3b2e7f1c9
85acead88180809d47524aac87d6f76799e7c0a1729d9614446be73aa8e7d871
0bbdb062ecfae7e1b59084a5e5fe052908ecfdea7db0777a9c318e9e55fdb5ff
77a1f62dc76cc9ee2d924008a0fdcc329396021f027ebe1cfa468f9625c2455b
8d11635019b077d36ce7de2a3ca9261f126e0ff5808f722fcb967e7cd000be23
519b2d04e80c2cb7c000a3c00cb30098df363bd825281b2b7384d964b832df3b
7a571f666c8f272cce1ee7ad75520a013bbed800e7d0c80a17804500a3474a13

A complete list of IoCs can be found at the following URL: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

Recommendation

It is recommended to apply a search on the systems for known indicators of compromise to make sure that the system was not exposed to these attacks. Please apply all available patches. Further, WAFs and other network filtering may help to prevent these sorts of attacks.

Patch URL

https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

Reference

https://www.bleepingcomputer.com/news/security/new-botnet-targets-network-security-devices-with-critical-exploits/

F5 BIG-IP PLATFORM VULNERABILITIES

F5 specializes in application services and helping organizations with scalability. F5 offers various services, which include BIG-IP and BIG-IQ. BIG-IP is a collection of software and hardware-related services that provides performance, availability, and security. BIG-IQ is a software suite that monitors the health of the platform of application delivery and security and is the centralized management tool for BIG-IP.

Affected Systems

- BIG-IP - 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3, and 11.6.5.3 versions
- BIG-IQ - 8.0.0, 7.1.0.3, and 7.0.0.2 versions

Vulnerability Overview

There are critical vulnerabilities with various BIG-IP versions and a pre-auth remote execution flaw within a few BIG-IQ versions. Successful exploitation of these vulnerabilities could allow attackers to fully take over these vulnerable systems or even lead to a DoS attack which could take the systems offline.

The vulnerabilities were discovered because of continuous security testing, and according to F5, there has not been evidence of public execution of these security flaws.

Attached will be another link that covers the vulnerabilities of F5 for March:
https://support.f5.com/csp/article/K02566623

Recommendation

Install the latest security patch is the only noted mitigation for this issue.

Reference

https://thehackernews.com/2021/03/critical-pre-auth-rce-flaw-found-in-f5.html

MALICIOUS WEBSITES ARE USING JAVASCRIPT TO EVADE VIRTUAL MACHINE

Phishing websites are now using JavaScript to detect virtual machine visitors and evade scans from said virtual machines. If the website sees a virtual machine, it will render a blank page. Otherwise, it will generate its actual phishing landing page. This new technique stems from the fact that many cybersecurity teams use virtual machines to scan potentially malicious websites.

Affected Systems

- Virtual machines

Vulnerability Overview

The JavaScript code checks the screen dimensions of the visiting machine. It queries the machines rendering software through WebGL API because software rendering is commonly found on virtual machines (SwiftShader, VirtualBox, LLVMpipe, etc.). The code also checks if the color depth of the machine's screen is 24-bits or less. If any of these are found by the code, a blank page will be rendered.

The code used in this detection and evasion appears to come from the URL listed below:

https://bannedit[.]github[.]io/Virtual-Machine-Detection-In-The-Browser.html

Recommendation

Use virtual machines with standard screen sizing and a regular hardware rendering engine.

Reference

https://www.bleepingcomputer.com/news/security/phishing-sites-now-detect-virtual-machines-to-bypass-detection/

MICROSOFT TEAMS AND SHAREPOINT FILES DELETED FOLLOWING RECENT OUTAGE

Organizations that use Microsoft Teams and SharePoint have reported that their files have gone missing or moved to the recycling bin following the most recent outage this past Monday. Microsoft has confirmed that nearly all cloud services were affected, including Outlook.com, SharePoint, Teams, Exchange Online, and Xbox Live. Microsoft has acknowledged that this outage was due to Azure Active Directory configuration issues.

Affected Systems

- A majority of Microsoft's cloud services

Vulnerability Overview

Organization administrators who have received and investigated their client's SharePoint environment have noted that the folder structure remained unchanged, but all of the files were missing. After investigation, administrators usually find that these files are now in the local recycle bin or SharePoint's Cloud Recycle Bin. Some administrators reported changing user passwords to prevent files from being deleted.

Free users of Microsoft Teams have reported that shared files are no longer able to be opened on any device. Microsoft stated that the cause was found, and patches were in the works but did not share the cause.

Microsoft Advisories:

SP244708 (SharePoint)
OD244709 (OneDrive)

Recommendation

Retrieve missing files from the appropriate recycle bins and apply patches as released.

Reference

https://www.bleepingcomputer.com/news/microsoft/mysterious-bug-is-deleting-microsoft-teams-sharepoint-files/

OLD LINUX STORAGE TECHNOLOGIES RECEIVE NEW PATCHES

Researchers at GRIMM recently uncovered an interesting series of vulnerabilities in Linux. While the CVSS scores are not critical (7.0 using CVSS 3 metrics), the fact they affect older hardware is interesting. SCSI and iSCSI drives have largely been replaced with newer storage methodologies and hardware but still, see plenty of use in the wild. As such, sometimes the older bugs are the most pertinent.

Affected Systems

- Linux

Vulnerability Overview

The bugs, covered by CVE-2021-27365, CVE-2021-27363, and CVE-2021-27364, are not overly easy to exploit. However, they can be used for a variety of purposes. The issues reside primarily on Linux servers with Remote Direct Memory Access in use. This is a streamlining technology and where the

issues reside. The researchers released a proof of concept (POC) for the exploits, which shows how to exploit the code in question. Particular distributions, such as CentOS, Red Had Enterprise Linux (RHEL), and Fedora, are particularly susceptible as unprivileged users can load the required modules if the rdma-core packages are enabled.

Recommendation

These issues have been patched. As such, we recommend testing and patching as soon as is practical, given a proof-of-concept is available for the exploit.

Reference

https://www.zdnet.com/article/old-linux-storage-bugs-new-security-patches/

THE TOP 10 HACKER-FRIENDLY USERNAMES AND PASSWORDS THAT YOU SHOULD NEVER EVER USE

Broken authentication is the second most common web application attack according to the 2020 OWASP Top 10 list, which should be considered the highest priority by every member of the information technology workforce, especially C-level or admin-level cybersecurity professionals. When authentication processes are not appropriately configured, adversaries will have a greater chance of intruding into your systems and compromising your assets.

Cyber threat actors are looking to optimize their work to compromise the highest number of systems possible and increase their profits. Their primary focus is to find the easiest and fastest way to break the walls of your cyber defense.

Affected Systems

- Corporate Networks

Vulnerability Overview

Attackers prefer to focus on SSH brute-forcing attacks when compared to the other techniques. For example, should the attack volume be considered, SSH Brute forcing attempts to administrative logins are observed 2.7 times more frequently when compared to the HTTP attacks and three times more common than Telnet attacks which are primarily used in IoT devices. Why do the adversaries like SSH attacks? Because most of the service applications keep using SSH protocol over port 22 for remote administration and require sys-admin level access instead of user access. Moreover, another common threat to our network security is that the vendor credentials are left unchanged since it provides an easy way for them to access the system for the service. However, it is also known to be low-hanging fruit for the adversaries who can make an easy google search for the default vendor credentials and just use it to access through your gateways.

The most popular attacked SSH username is known to be "root" since it is the most common vendor default username used in Unix-based systems (Applications, services, IoT devices, all network devices), and it is used three times more than the second hacker-friendly username "admin". All the usernames

and passwords below are a massive risk for your organization, and they should be replaced with strong credentials as soon as possible.

#	Username	Password
1	root	admin
2	admin	admin
3	user	user
4	test	test
5	ubuntu	ubuntu
6	ubnt	ubnt
7	support	support
8	oracle	oracle
9	pi	raspberry
10	guest	guest

Recommendation

The first critical action you may take after reading this advisory report is checking for SSH access to any applications/services not only on your perimeter but also on your LAN and WiFi accessible devices. Replace the top attacked credentials in your system with the strong credentials at the earliest time possible. Check for the default credentials in your system, especially those with admin privileges, and change them as soon as possible.

Enforce strong credential management in your workplace, implement MFD (multifactor authentication), monitor failed login attempts for abnormal patterns, and implement secure session management are further recommendations.

Reference

https://www.f5.com/labs/articles/threat-intelligence/spaceballs-security--the-top-attacked-usernames-and-passwords
https://snyk.io/learn/owasp-top-10-vulnerabilities/