BRAINTRACE

THREAT ADVISORY REPORT

APRIL 8,2021

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.

TOP DATA BREACH ROOT CAUSES AND PATCH MANAGEMENT

Almost 60% of data breaches in recent years were reported to be related to the lack of best practice in patch management, according to the 2020 Cyber Hygiene Report contributed by 560 IT professionals from the organizations with 500 to 25,000 employees and published by Automox. Root causes reported by the 81% of the participants who faced a data breach problem in the last 24 months were listed as follows:

- Phishing attacks (36%)
- Missing OS patches (30%)
- Missing Application patches (28%)
- Misconfiguration of OSs (27%)
- Insider threat (26%)
- Credential theft (22%)
- Brute force (17%)

This study's most interesting finding was the surprisingly high percentages of patch mismanagement and misconfigurations in data breaches. We can conclude that one of the best hardening methods of our defense against cyberattacks is having a solid patch management procedure in place since missing OS patches are known to be the number 1 technical attack surface exposure to cause a data breach.

Another interesting finding of the study is about the patching times of the participants. Unfortunately, few entities are fast enough in patch management. Less than 50% of the responding organizations reported that they could complete the patching for critical vulnerabilities with a CVSS score of 9-10 in less than three days. Only 20% said they could respond to zero-day vulnerabilities within 24 hours. Moreover, 15% of the systems were reported to be unpatched after 30 days.

Affected Systems

- All Systems

Vulnerability Overview

Patch management is not a trivial task since more than 10.000 vulnerabilities per year are being published and waiting for patching as soon as possible. Prioritization and planning are very critical steps to overcome the complexity of the vulnerability management process. The major problems faced by companies in patch management are reported to be:

- Remote users and systems
- Inefficient testing of patches
- Lack of visibility for the endpoint devices

- Lack of a centralized and automated patch management system
- Insufficient staffing

Recommendation

Prioritize your patches based on their criticality levels and conduct appropriate testing. Further, Patch Management systems are an excellent tool to help automate many of these functions.

Reference

https://www.darkreading.com/vulnerabilities---threats/missing-patches-misconfiguration-top-technical-breach-causes/d/d-id/1337410

https://patch.automox.com/rs/923-VQX-349/images/Automox_2020_Cyber_Hygiene_Report-What_You_Need_to_Know_Now.pdf

INFORMATION ABOUT 533 MILLION FACEBOOK USERS LEAKED ON CYBERCRIME FORUM

Hackers published the phone numbers and account data of 533 million Facebook users. Account data includes job description, location, profile names, gender, email, Facebook ID, and much more info users entered on their social network. All this stolen data is separated into 106 download packages, and they are organized by countries. The forum where these packages were posted is public, but if malicious actors want to download them, they need to buy forum credits. Facebook confirmed that this is old information and that the case was resolved in August 2019.

Affected Systems

- Facebook

Vulnerability Overview

Countries impacted include the United States, U.K., Canada, Australia, and more. This data is used as a backend of a Telegram bot that was published beginning of 2021. There is a big chance that malicious actors will use this information to execute extortion, threats, SMS spam, Robocalls, and many more. The United States has 32,315,282 accounts exposed in this.

Recommendation

Please make sure that passwords need to be strong and updated regularly. We recommend not sharing too much information about your verification and data on the profile. Following up with recent news on the Facebook incident will contribute mitigation.

Reference

https://www.zdnet.com/article/facebook-data-on-533-million-users-posted-online/

BAD ACTORS USE WINDOWS OS FEATURE TO EVADE FIREWALL AND GAIN PERSISTENCE

A new technique adopted by bad actors leveraging Microsoft Background Intelligent Transfer Service (BITS) to secretly deploy malicious payloads on Windows systems is surging. FireEye's Mandiant cyber forensics arm has discovered an unknown persistence component showing adversaries using BITS to launch backdoor attacks.

Affected Systems

- Windows

Vulnerability Overview

BITS is a Microsoft Windows component that was introduced in Windows XP. It makes use of idle network bandwidth to help transfer asynchronous files between machines. This happens when a job is created when a container has the files to download or upload. BITS is primarily used to deliver OS updates to clients and Windows Defender antivirus to retrieve malware updates.

To avoid malicious attempts being detected and blocked by the firewall, files are downloaded or uploaded in the service host process context when the malicious application creates BITS tasks. After the system is compromised, Ryuk malware is found to use the BITS service and create a system update job that is already set up to launch mail.exe and open the door for the KEGTAP backdoor after trying to download an incorrect URL. The malicious BITS task is set up for HTTP transfer of a nonexistent file from the host computer. BITS would set off the error state and start the notify command, which is the KEGTAP backdoor.

Recommendation

To prevent backdoor attacks, you should install a powerful antivirus with malware detection and prevention capabilities, a firewall, and a network monitoring tool. Regular system patching is also recommended.

Reference

https://thehackernews.com/2021/04/hackers-using-windows-os-feature-to.html

VMWARE CARBON BLACK CLOUD VULNERABILITY PATCHED

A vulnerability was found in VMware's Carbon Black Cloud Workload, designed to secure workloads, vulnerability management, antivirus replacement, and risk and compliance. A specific URL that is vulnerable to manipulation and related to the administrator interface of Carbon Black Cloud could allow attackers to bypass authentication.

Affected Systems

- VMware Carbon Black Cloud Workload products not updated with the latest version releases

Vulnerability Overview

An attacker can access Carbon Black Cloud's administrator API with network access to the administrator interface after obtaining an authentication token, resulting in read and write capabilities regarding configurations.

Recommendation

Apply the latest version releases by VMware.

Patch URL

https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.0/rn/cbc-workload-102-release-notes.html

Reference

https://www.vmware.com/security/advisories/VMSA-2021-0005.html

HACKERS SET UP A FAKE CYBERSECURITY FIRM TO TARGET SECURITY EXPERTS

Hackers are now setting up to target Cybersecurity researchers yet again. Google has discovered a website for a fake company named SecuriElite. Not only is there a website for this company, but they have begun setting up different profiles on platforms such as Twitter, Discord, and LinkedIn. There have already been two LinkedIn accounts tagged for impersonating recruiters for antivirus and security companies.

Affected Systems

- Media platforms such as Discord, Twitter, and LinkedIn

Vulnerability Overview

Attackers today are using more and more different ploys to attack their victims. This most recent one is not new and has been tried before. The attackers, however, are getting better in how they portray themselves and where they take their social-engineering ploys. The same North Korean threat actors that targeted researchers in January have been seen readying a new campaign. SecuriElite, located in Turkey, claims to offer pen-tests, software security assessments, and exploits. There have been indications that this company and the associated websites and profiles are fake. These appear to be linked to the notorious threat group Lazarus. The attackers will contact the researcher, asking if they want to collaborate on vulnerability research together. Attackers will provide the victims with malicious Twitter links or even send a malicious code within a Visual Studio Project that can install a backdoor within their system. It is thought that these attacks will be used to uncover and steal vulnerabilities to use in North Korean APT campaigns.

Recommendation

Researchers found that those infected were running fully patched and updated Windows 10 and Chrome browser versions. It is recommended that users continue to keep their devices updated to the current operating systems. Users should also make sure they have antivirus or antimalware protection on their phones and tablets like they do on their computer systems.

Reference

https://threatpost.com/north-korean-apt-security-researchers/165155/

VMWARE'S VREALISE OPERATIONS RECEIVED PATCH

vRealize Operations is a suite of IT Management tools used for a variety of cloud environments. VMWare describes the software as AI-powered and "self-driving," in reference to Tesla's line of automobiles. That said, Positive Technologies researcher Egor Dimitrenko isolated a credential-stealing flaw in the software for which VMware recently released a patch.

Affected Systems

- VMware vRealize Operations
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager

Vulnerability Overview

The issue covered by CVE-2021-21975 is a server-side request forgery bug in the vRealize Operations Manager AI. This issue can be exploited without requiring authentication or user interaction. The attack is relatively simple and allows would-be hackers to steal administrative credentials. VMware gave the bug an 8.6 out of 10 utilizing CVSS 3.0 metrics.

Recommendation

If you are affected by this issue, it is recommended to patch as soon as possible. If you cannot expediently patch the problem, you can execute a workaround via removing a line from the casa-security-context.xml file and restarting the CaSA service. Details are in the security links for the products specified.

vRealize Operations 7.5: https://kb.vmware.com/s/article/82367
vRealize Operations 8.0.1: https://kb.vmware.com/s/article/83093
vRealize Operations 8.1.1: https://kb.vmware.com/s/article/83094
vRealize Operations 8.2: https://kb.vmware.com/s/article/83095
vRealize Operations 8.3: https://kb.vmware.com/s/article/83210

Reference

https://www.bleepingcomputer.com/news/security/vmware-fixes-bug-allowing-attackers-to-steal-admin-credentials/

NEW BUGS ON LINUX SYSTEMS COULD LET HACKERS BYPASS SPECTRE ATTACK MITIGATIONS

Two weeks after Google has published a proof-of-concept (POC) to demonstrate the Spectre attack in a web browser, Piotr Krysiuk of Symantec's Threat Hunter team has discovered two flaws in Linux Systems that could let malicious actors bypass Spectre Attack mitigations and steal kernel memory's sensitive information. The flaws are tracked as CVE-2020-27170 and CVE-2020-27171.

Affected Systems

- Linux

Vulnerability Overview

All Linux kernels before 5.11.8 patches are impacted by these two new bugs. New patches to fix the vulnerability were released on March 20th for Ubuntu, Debian, and Red Hat distributions.

The new flaws uncovered by the security researcher aim to bypass mitigations in Linux by leveraging the kernel's support for extended Berkeley Packet Filters (eBPF) to pull out the contents of the kernel memory. BPF running on affected systems could bypass Spectre mitigations, perform insecurely out-of-bounds loads with no restrictions, and expose kernel memory contents via side-channel attacks.

The kernel ("kernel/bpf/verifier.c") can execute unpleasing out-of-bounds on pointer arithmetic and fails the fixes for Spectre attack.

The flaws could also be exploited if a bad actor can access the affected machine via malware download and gain remote access. This can allow bad actors to use these vulnerabilities and access all users' profiles on the affected device.

Recommendation

Apply the patches to mitigate the risk associated with the vulnerabilities.

Reference

https://thehackernews.com/2021/03/new-bugs-could-let-hackers-bypass.html

LIBCURL URL STRIPPING VULNERABILITY IN THE PROCESS OF BEING PATCHED

Libcurl is a client-side URL library and command-line tool that transfers data using network protocols. It supports the following protocols: Dict, FTP, FTPS, FILE, HTTP, HTTPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet, TFTP, IMAP, IMAPS, LDAP, LDAPS, and Gopher.

Affected Systems

- Curl versions 7.1.1 to 7.75.0

Vulnerability Overview

Libcurl fails to remove user credentials from URLs during the automatic population of the HTTP request header field "Referer:" in outgoing HTTP requests. This vulnerability could lead to data leaks regarding the target server of the secondary HTTP request.

Recommendation

Update curl versions as soon as available for the affected OS.

Patch URL

https://curl.se/XOXep4o2CSG0.patch

Reference

https://ubuntu.com/security/CVE-2021-22876

ACCUSOFT IMAGEGEAR CUSTOMERS UNDER ATTACK

A discovery in Accusoft's Image Gear software has been recently uncovered with Cisco Talos' help, in which an attacker could exploit and corrupt the internal memory of a targeted machine. Access is the derivative of the activation of a maliciously created file. Image Gear is a popular resource for developing, creating, imaging, and editing documents; and is frequently shared via DICOM, PDF, Microsoft Office, and many other methods.

Affected Systems

- Accusoft ImageGear version 19.8

Vulnerability Overview

Below is a quick list of the vulnerabilities:

- CVE-2021-21773 - Out-of-bounds write vulnerability that exists within the TIFF header count-processing function. Actions are committed through an attacker-crafted file made to produce memory corruption.
- CVE-2021-21776 - Out-of-bounds write vulnerability exists in the SGI Format Buffer Size Processing function. Vulnerability also exists due to the memory corruption results of the received malicious file.
- CVE-2021-21782 - Out-of-bounds write vulnerability targeting the SGI format buffer size processing functionality. An attacker can provide the familiar file to trigger this memory corruption vulnerability.

Recommendation

Cisco Talos and Accusoft have both confirmed that a relevant patch had been released to handle the matter. Affected or exposed customers are urged to download the newest patch when possible.

Reference

https://blog.talosintelligence.com/2021/03/vuln-spotlight-accusoft-image-gear-march-2021.html?&web_view=true

PATH TRAVERSAL VULNERABILITY FOUND IN CISCO HOSTING ENVIRONMENTS

Cisco IOx is a hosting environment used for managing IoT technology. A vulnerability was found in products when integrated with Cisco IOx that could allow malicious parties to conduct remote, unauthenticated directory traversal attacks and modify OS and host files.

Affected Systems

- 809 Industrial Integrated Services Routers - 15.8(3)M2 and later, earlier than the first fixed release.
- 829 Industrial ISRs - 15.8(3)M2 and later, earlier than the first fixed release.
- CGR 1000 Compute Module - 1.9 and later, earlier than the first fixed release.
- IC3000 Industrial Compute Gateway - All releases earlier than the first fixed release.
- Devices running Cisco IOS XE Software - 16.11.1 and later, earlier than the first fixed release.

Vulnerability Overview

This vulnerability stems from improper URL validation in Cisco IOx API requests. Crafted API calls from malicious parties containing directory traversal characters could successfully exploit this vulnerability. Malicious parties would then go on to modify OS files of the host system.

Recommendation

Update affected products to the latest releases available.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-pt-hWGcPf7g

PHP'S GIT SERVER INFILTRATED WITH BACKDOOR MALWARE

PHP's official Git server was hacked by two threat actors in a software supply chain attack that has yet to be identified. The threat actors inserted unauthorized updates to PHP's source code, injecting backdoor malware. PHP has since reverted the updates and is investigating their repositories for any compromise or malicious activity indicators. The PHP team has announced several changes to increase PHP's security, including moving the source code repository to GitHub and requiring developers to be added to an organization on GitHub.

Affected Systems

- Systems using PHP's official Git server

Vulnerability Overview

The hack that infiltrated PHP's source code were two malicious commits executed on the "php-src" repository that is hosted on the git[.]php[.]net server. This indicates that the git.php.net server was compromised versus just a single get account, according to developers. The two changes were committed as a "Fix Typo" in an attempt to evade detection and included provisions for the execution of arbitrary PHP code. The malicious commits executed code from the useragent HTTP header. The string started with 'zerodium.' Zerodium is a zero-day exploit known for having high-impact and high-risk vulnerabilities in software.

Recommendation

It is recommended to have strong security practices, include Secure development techniques, code review and storage, and hashing known good code and file samples to establish necessary baselines to work from, if required.

Reference

https://thehackernews.com/2021/03/phps-git-server-hacked-to-insert-secret.html

MULTIPLE BACKDOORS TARGETING INDUSTRIAL SECTORS IN JAPAN

On March 30th, 2021. Kaspersky researchers have discovered details of a cyberattack campaign that aimed to install malicious backdoors to swipe information from several industrial sectors in Japan.

Affected Systems

- Windows

Vulnerability Overview

Kaspersky researchers named this backdoor "A41APT". This A41APT attack is undertaken by APT10 (Stone Pando or Cicada) using malware to transfer payloads (SodaMaster, P8RAT, and FYAnti).

The attack leverages a multi-stage attack process. The intrusion first abuses SSL-VPN and exploits unpatched vulnerabilities or stolen passwords. This campaign's core is a malware called Ecipekac that crosses a four-layer loading scheme and uses the four files to load and decrypt four fileless loader modules until the final payload is loaded into memory.

P9Rat and SodaMaster payloads are mainly used to download and execute payloads retrieved from the servers controlled by threat actors. According to Kaspersky, they have not released any information about which malware affects the target Windows machines. The third payload, FYAnti, is a multi-layer loader that installs a final-stage remote access trojan (QuasarRAT) by going through two more consecutive layers.

This cyber-attack avoids detection by using fireless implants, obfuscation, anti- VM, and remove activity logs.

Recommendation

To prevent backdoor attacks, you should install a powerful antivirus with malware detection and prevention capabilities, a firewall, and a network monitoring tool.

Reference

https://thehackernews.com/2021/03/hackers-are-implanting-multiple.html

ROBINHOOD TAX SEASON PHISHING

The month of April is usually when taxes are due, but they are due in May this year. Malicious attackers capitalize on significant events, holidays, or trends in the media or world to take advantage of people. In this case, attackers target Robinhood users with phishing emails trying to extract confidential information from users. Robinhood has existed for a couple of years, and their main goal is to help their users to buy and sell stocks, but it looks like this year, attackers are willing to take advantage of tax season.

Affected Systems

- Robinhood Users

Vulnerability Overview

Robinhood users were targeted through phishing emails that would link the user to fake Robinhood sites. From these sites, the attackers attempt to extract information from the unexpected user.

An attacker would target Robinhood users to tempt the user to download tax files with malware encoded with the download.

Recommendation

Robinhood has suggested that users download the app from either the Google play store or IOS store and access tax files through the app or their verified site.

Reference

https://threatpost.com/robinhood-warns-customers-of-tax-season-phishing-scams/165180/?web_view=true

NEW RANSOMWARE VICTIM IS A CYBER INSURANCE PROVIDER: CNA-CONTINENTAL NATIONAL AMERICAN GROUP DATA BREACH

A sophisticated ransomware attack hit the seventh biggest insurance company globally with 5,800 employees on March 21, 2021. The cyberattack on CNA's network resulted in disruption in their network and impacted some critical systems, including corporate emails, according to the statement by the Chicago-based company. This cyberattack utilized a new version of the Phoenix CryptoLocker malware known to encrypt the files immediately and request a ransom from the victims to provide the decryption key. CNA has declared that they have disconnected their systems from their network, which continue to function. The Insurance Giant is reported to be planning to restore its systems using its' backups instead of paying the ransom. CNA has declared on its website that it is working with third-party forensic experts and law enforcement officials to determine the full scope of this incident.

Affected Systems

- CNA's Network

Vulnerability Overview

There are currently no PoC exploits available to the public, and specific technical details have not been released at this date. It's reported that the insurance giant was hit with a variant of the Phoenix CryptoLocker malware, though specific indicators of this malware are unknown at this time.

Recommendation

Every business in any type of industry can be a victim of cybercrime, and the best protection against it is to apply the core security practices such as:

- Continuous education and training of the employees
- Using licensed products
- Patch Management
- Using reputable antivirus solutions
- Turning on the spam filters on your emails
- Using allow-lists

- Strong Backups
- Segmentation (LANs, VLANs)
- Strong IAM-Identity & Access Management

Reference

https://threatpost.com/cna-hit-novel-ransomware/165044/

https://www.cnasurety.com/

https://grahamcluley.com/cyber-insurance-giant-cna-hit-by-ransomware-attack/

TRUSTWAVE UNCOVERS VULNERABILITY IN POPULAR WEBSITE CMS UMBRACO

A Cybersecurity agency Trustwave recently found a safety vulnerability in CMS, Umbraco. Researchers have outlined situations of a privilege escalation situation within their report. This situation would allow low privilege customers to raise their status to Admin. Umbraco is an open-source content management system platform for publishing on the web. It is written in C# and deployed on Microsoft-based infrastructure.

Affected Systems

- Umbraco variations 8.9. zero and eight.6.3.

Vulnerability Overview

A vulnerability that resides within an API endpoint does not check the user's authorization properly before returning results found to the application's logging section. Trustwave concluded that this was because the LogViewerController class does not use granular authorization attributes on the exposed endpoints. Because of the exposed endpoints, lower privileged users are given higher privileges.

Recommendation

It is recommended that users keep their devices updated to the current operating systems. This will make sure that all security patches are present and installed. Users should also make sure they have antivirus or antimalware protection on their devices as they do on their computer systems.

Reference

https://thecybersecurity.news/general-cyber-security-news/trustwave-uncovers-vulnerability-in-popular-website-cms-7774/

PHISHING ATTACKS USING VACCINE SURVEYS

The Department of Justice published a warning regarding an active phishing campaign. These phishing scams are sending fraudulent COVID-19 vaccine surveys. They are being sent via emails and text messages. Fraudsters are manipulating victims to click on the link with a promise that they will earn exclusive awards like iPad Pro after they fill out the survey. They were asked to provide payment for shipping and handling fees.

Affected Systems

- Email
- Text message

Vulnerability Overview

By providing personal identification information, they gave scammers information that can easily be used for identity theft. Since victims entered complete credit card information, this can be valuable data for fraudsters to earn monetary gain. Emails usually look like they were sent from the government or financial institutions, or social media platforms. These scams are sometimes hard to notice since emails can look trustworthy. The best practice is to double-check the sender and never click on the links provided.

Recommendation

The Department of Justice recommends that if you receive one of these emails or text messages with surveys about COVID 19 and provided link, you should report it to the National Center for Disaster Fraud (NCDF) by calling 866-720-5721 or via the NCDF Web Complaint Form at the URL below:

http://www.justice.gov/disaster-fraud

The best way to protect yourself is to be educated on common scams and be careful before clicking on the links asking you to complete some action. Basic information about scams and how to protect yourself can be found the URL below:

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

Reference

https://www.bleepingcomputer.com/news/security/us-doj-phishing-attacks-use-vaccine-surveys-to-steal-personal-info/

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

NPM NETMASK PACKAGE VULNERABILITY

GitHub is a place where software developers can host and share their software with others to use. Various projects are hosted on GitHub, such as projects that can help a company with networking. NPM Library Netmask is a package that can be downloaded from GitHub and used in an organization's code to help resolve IP addresses over the internet. The vulnerability discovered with this package is associated with the sanitization of how the package resolves IP addresses.

Affected Systems

- Netmask NPM versions < 2.0.0

Vulnerability Overview

Security researchers discovered that this issue involves the IPv4 octets and how the package tries to resolve a given IP. An IP address can be represented in different formats such as hexadecimal or integer. An IP address can be represented as 127.0.0.1, which would be in decimal format or presented in an octal format.

This can be an issue because if an attacker would be able to prefix a zero to an IP, this can change the IP address and put in an IP range that could be allowed through an organization's firewall. Other vulnerabilities that can occur because of this bug could be remote file inclusion or server-side request forgery, but this bug has been resolved in the latest version of this package.

Recommendation

Update to version 2.0.0.

Reference

https://portswigger.net/daily-swig/ssrf-vulnerability-in-npm-package-netmask-impacts-up-to-279k-projects#:~:text=Netmask%2C%20which%20is%20used%20to,end%20projects%2C%20according%20to%20Codes.

STATE HACKERS ATTACK FORTINET FORTIOS SERVERS

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) published warning that malicious actors are actively attacking Fortinet FortiOS serves by exploiting its vulnerabilities. Vulnerabilities that the state hackers are using are CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591. Hackers are attacking unpatched servers and conduct scanning across ports 4443, 8443, and 10443.

Affected Systems

- Fortinet FortiOS

Vulnerability Overview

Advanced persistent threat (APT) actors exploit these system weaknesses to access the victim's network. These bugs can be used for future attacks and breaches. It is known that APT actors, after earning privileged access, position themselves for successful execution of DDoS, ransomware, and SQL injection attacks. These attacks impacted commercial, government, and tech institutions.

Recommendation

Please patch listed vulnerabilities to mitigate any malicious actions on your system. It is recommended to regularly update your data and protect it adequately. Multifactor authentication and network segmentation can highly contribute to the cyber safety of every organization.

Patch URL

https://www.ic3.gov/Media/News/2021/210402.pdf

Reference

https://www.bleepingcomputer.com/news/security/fbi-and-cisa-warn-of-state-hackers-attacking-fortinet-fortios-servers/

BEST PRACTICES FOR PATCH MANAGEMENT

The importance of patch management keeps increasing in direct proportionality with the volume of cybercrime. Remediation of reported vulnerabilities by applying security patches and keeping your software up to date has never been so necessary. Patch management on any software, including the operating systems (OS), applications, or browsers, are done for three fundamental reasons:

1. Remediating the security weaknesses in your systems before the cyber threat actors
2. Remediating the functional bugs
3. Maintaining regulatory compliances and staying away from the fines resulting from violations of related industry standards.

What are the major benefits of patch management?
1. Improved security,
2. Minimized downtime that cyberattacks or functional bugs may cause,
3. Reduced compliance fines.

Affected Systems

- All Systems

Vulnerability Overview

Some common questions to ask:

How much time do you have for Patch Management?

It is highly recommended to complete the patches in 30 days, but always keep in mind the basic rule "the earlier, the better" to protect your network from any kind of cyberattacks and before threat actors.

What are patch management best practices to successfully implement an efficient patching process?

- Know and control your inventory, including all types of devices, software, operating systems, and third-party applications. Many successful cyberattacks have been reported utilizing systems neglected by IT.
- Categorize or prioritize your inventory and users, then plan patching based on their criticality levels.
- Centralize your patching procedures using a single console.
- Monitor for new vulnerabilities and patch releases regularly. Always get patches from original vendor sites.
- Automate the patch management process to decrease the time between the release and application of patches.
- Complete your backup and test the patches in a testing environment before deploying them to production systems to avoid unforeseen issues.
- Validate that patches work as expected and don’t cause any unexpected problems in your systems or applications.
- Standardize the patching process by establishing policies like what will be patched, when, under what conditions.
- Document and report any changes via patch management procedures have been carried out.

How frequently should security-related vulnerabilities be patched?

The total number of software vulnerabilities has been reported to be more than 18.000 for the last year, while those at critical levels, such as "remote code execution," were detected to be more than 4300. Given those numbers, the critical vulnerabilities should be remediated as soon as possible.

What is the relationship between data breaches and patch mismanagement?

Almost more than half of all security breaches are reported to have happened due to the exploitation of a known vulnerability that could be easily patched, according to a Ponemon Institute Report.

Recommendation

Regardless of the system you use for Patch Management, verify the reports presented to you with vulnerability testing and other methods to ensure systems are patched. Client-based patching is usually recommended, as noted in the information above, as this can usually be controlled via a central console.

Further, ensure your patching falls within your organization's maintenance windows. As system version upgrades and cumulative patches can take a long while to process on the endpoints within your organization's environment, please ensure your maintenance window provides adequate time for the patch process to complete.

Reference

https://www.kaseya.com/blog/2021/03/09/patch-management/

https://www.ninjarmm.com/blog/patch-management-process/

BAZARCALL MALWARE USES MALICIOUS CALL CENTERS TO INFECT VICTIMS

There has recently been an ongoing battle against a new version of the BazarCall malware. This malware is now using call centers to assist in distributing its extremely damaging malware. It was first discovered back in early January being sent by call centers. A fictitious company will send out an email to the victim asking them to call a number instead of clicking on an embedded link within the email.

Affected Systems

- Machines running Windows Operating Systems are the systems most in danger. "BazarCall" can distribute some of the most damaging Windows malware.

Vulnerability Overview

Attackers today are using more and more different ploys to attack their victims. This recent ploy has victims calling a number within an email to cancel a subscription. The victim will see a phishing email usually directed at corporate users, stating that the "free trial" is over. The emails will not provide details regarding the subscription. They are given a phone number to contact, or they could be charged $69.99 to $89.99 as a renewal charge. When the victim calls the number, they will give a "customer ID." If that customer ID is correct, the victim will be directed to a fake website associated with the company and prompted to download an Excel document. Once the Excel document is downloaded, and the victim clicks on the "Enable Content," the malware begins to download. Due to researchers' and analysts' efforts, these groups constantly have to change the phone numbers, and even the hosting sites for they are getting taken down. The problem is that until the victims stop falling for this scam, they will continue this delivery method.

Recommendation

It is recommended that users keep their devices updated to the current operating systems. This will make sure that all security patches are current and installed. Users should also make sure they have antivirus or antimalware protection on their devices like they do on their computer systems. If a download or a program requests you to turn off this protection, please do not do it.

Reference

https://www.bleepingcomputer.com/news/security/bazarcall-malware-uses-malicious-call-centers-to-infect-victims/

CALL OF DUTY CHEATS EXPOSE GAMERS TO MALWARE

The gaming world continues to be a honeypot for attackers looking for a payday. In 2020 alone, more than 61% of the gamers out there reported that some sort of scam had targeted them. These malicious actors' tactics can be anything from fake APK's of the mobile games to compromise player's accounts to publish on other malicious sites.

Affected Systems

- Call of Duty: Warzone video game on various platforms.

Vulnerability Overview

Activision has issued a warning to its game users regarding a new threat towards the famous game Call of Duty: Warzone. There is an ad for cheat codes that a threat actor has started publishing to get the victim to install its Remote Access Trojan (RAT). These ads will convince users that they have a free cheat code that will assist them in the popular gameplay. When installing a cheat program, it is not uncommon for the user to be asked to disable their antivirus, firewalls and even disable kernel code-signing and other security programs. It is also not unusual for a cheat program to run. It needs to have the highest system privileges available to it.

This will be the first time that the malware being used has been identified. Researchers have named this piece of malware "COD-Dropper v0.1". As of March 1st of this year, the actors have even begun to post YouTube videos with step-by-step instructions on how to download the "cheat" This is a very simplistic method of delivering the malware, but it has been very effective.

Recommendation

It is recommended that players of the game avoid looking for cheat tools to assist in the game. It is also recommended that users have updated malware protection on their systems and ensure operating systems are running on the most current release.

Reference

https://threatpost.com/call-of-duty-cheats-gamers-malware/165209/

APACHE SPAMASSASSIN CODE EXECUTION

This critical code execution vulnerability was discovered and privately disclosed to Apache SpamAssassin by Damian Lukowski at Credativ before public disclosure on March 24. Apache is now urging users to avoid using configuration files from untrusted sources before applying the patch. The CVE was assigned a critical 9.8 severity CVSSv3.1 score by NIST NVD but is undergoing further analysis.

Affected Systems

- Apache SpamAssassin before version 3.4.5

Vulnerability Overview

A malicious Perl-based rule configuration .cf file can execute arbitrary commands on the system on a vulnerable version of Apache SpamAssassin. There are currently no PoC exploits available to the public, and specific technical details have not been released at this date.

Recommendation

Apply vendor-provided patches and only load configuration files from trusted sources.

Patch URL

https://spamassassin.apache.org/downloads.cgi

Reference

https://mail-archives.apache.org/mod_mbox/spamassassin-announce/202103.mbox/%3C241c47dc-467f-c622-c8ab-e06df159b475%40apache.org%3E

NEW ANDROID SPYWARE DISGUISED AS "SYSTEM UPDATE" DISCOVERED BY RESEARCHERS

Recently, researchers at Zimperium discovered a malicious spyware tool running on Android OS disguising itself as an app called "System Update." This spyware had nothing to do with updating the device, although it likely had that capability among many others. It is good to know that this malicious application was not downloaded on the Google play store. However, other malicious apps have done so in the past.

Affected Systems

- Androids

Vulnerability Overview

This application is a form of spyware that has wide-reaching surveillance functionality.

Recommendation

Do not download apps outside of trusted distribution apps or methods, such as Google Play Store, Apple Store, or your organization's app management portal.

Reference

https://techcrunch.com/2021/03/26/android-malware-system-update/?&web_view=true

TWO HIGH-SEVERITY SECURITY VULNERABILITIES PATCHED IN OPENSSL

OpenSSL maintainer released patches for the 2 High-Severity Security Vulnerabilities that could lead to denial-of-service (DoS) attacks and avoid certificate verification. They are tracked for CVE-2021-3449 and CVE-2021-3450 and fixed in the OpenSSL 1.1.1k update on March 25, 2021.

Affected Systems

- Applications that rely on a vulnerable version of OpenSSL

Vulnerability Overview

- CVE-2021-3449 - Affects all Open SSL 1.1.1 versions. This vulnerability concerns a potential DoS vulnerability because of the NULL pointer dereferencing that could affect an OpenSSL TLS server to crash during a renegotiation when a client transmits a malicious "Client Hello" between the TCP handshakes.
- CVE-2021-3450 - Affects OpenSSL versions 1.1.1h and newer. This vulnerability concerns the X509_V_FLAG_X509_STRICT flag that allows extra security checks of certificates in a certificate chain. By default, this flag is not set up; an error in this implementation meant that OpenSSL is incapable of checking that "non-CA certificates must not be able to issue a different certificate," following the certificate bypass. This results in the vulnerability preventing applications from denying TLS certificates that are not signed by a certificate authority.

Recommendation

Apply the patches to mitigate the risk associated with the vulnerabilities.

Reference

https://thehackernews.com/2021/03/openssl-releases-patches-for-2-high.html