QUALYSEC
BEYOND CYBERSECURITY

2024

APRIL 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com

☎ 865 866 3664

✉ contact@qualysec.com

Hackers Hijacked Notepad++ Plugin To Inject Malicious Code

Hackers have manipulated a popular Notepad++ plugin, injecting malicious code that compromises users' systems upon execution.

The AhnLab Security Intelligence Center (ASEC) researchers have revealed that the "mimeTools.dll" plugin, which is widely used, was modified to carry out the attack.

Notepad++, a text and source code editor favored by programmers and writers for its versatility and plugin support, became an unwitting vehicle for cybercriminals.

Malicious vs Legitimate Package

The altered "mimeTools.dll" plugin, a default component of Notepad++, was discovered to be masquerading as a legitimate package, deceiving users into downloading and installing the compromised version. The mimeTools plugin, known for its encoding functionalities such as Base64, is automatically loaded when Notepad++ is launched. Attackers exploited this behavior using a technique known as DLL Hijacking.

When Notepad++.exe is launched, the "mimeTools.dll" file is automatically loaded, triggering the activation of the embedded malicious code, without any further user action.

Source : https://cybersecuritynews.com/hackers-hijacked-notepad-plugin/

Hackers Use Weaponized PDF Files to Deliver Byakugan Malware on Windows

Due to their high level of trust and popularity, hackers frequently use weaponized PDF files as attack vectors.

Even PDFs can contain harmful codes or exploits that abuse the flaws in PDF readers.

Once this malicious PDF is opened by a user unaware of it, the payload runs and infiltrates the system.

Cybersecurity researchers at Fortinet recently identified that hackers have been actively using weaponized PDF files to deliver Byakugan malware.

Technical analysis

FortiGuard Labs discovered a Portuguese PDF file distributing the multi-functional Byakugan malware in January 2024.

The malicious PDF tricks people into clicking a link by presenting a blurred table.

This in turn activates a downloader that puts a copy (requires.exe) and takes down DLL for DLL-hijacking.

This runs require.exe to retrieve the main module (chrome.exe). In particular, the downloader behaves differently when called require.exe in temp because malware evasion is evident.

Source : https://cybersecuritynews.com/hackers-weaponized-pdf-files/

Multiple Chinese Hacking Groups Exploiting Ivanti Connect Secure VPN Flaw

Cybersecurity firm Mandiant has uncovered a series of sophisticated cyberattacks targeting Ivanti Connect Secure VPN appliances.

These attacks, attributed to multiple Chinese nexus espionage groups, exploit critical vulnerabilities to facilitate lateral movement and compromise Active Directory systems.

This article delves into the intricate details of the CVEs involved, the clustering and attribution of these attacks, the deployment of new TTPs and malware, and the implications of such breaches.

CVEs: The Gateway to Exploitation

The initial disclosure of CVE-2023-46805 and CVE-2024-21887 on January 10, 2024, marked the beginning of a series of incident response engagements by Mandiant.

These vulnerabilities, an authentication bypass and a command injection flaw, have been the focal points of exploitation attempts by suspected Chinese nexus espionage actors.

The exploitation of these vulnerabilities underscores the critical need for timely patching and the application of appropriate mitigations.

As per the latest report by Google, several Chinese hacking groups are currently leveraging the vulnerability in Ivanti Connect Secure VPN to carry out their malicious activities.

Source : https://cybersecuritynews.com/chinese-hacking-groups-vpn/

Magento Vulnerability Let Attackers Inject Backdoor On E-commerce Websites

A sophisticated vulnerability within the Magento ecommerce platform has been unveiled, posing a significant threat to online merchants and shoppers alike.

The vulnerability, identified as CVE-2024-20720, allows attackers to inject a persistent backdoor into Magento servers, compromising the security of countless ecommerce websites.

The method of attack involves a clever manipulation of Magento's layout template system.

Attackers have been found to insert malicious XML code into the layout_update database table, which is then executed every time a customer accesses the checkout cart.

This execution relies on the combination of Magento's layout parser with the beberlei/assert package, a component installed by default on Magento systems.

The specific command executed, sed, is used to add a backdoor to the CMS controller, ensuring that the malware is re-injected even after manual fixes or system recompilations.

Malicious Payloads Injection

This backdoor not only allows attackers to maintain access to the compromised systems but also facilitates the injection of additional malicious payloads.

Source : https://cybersecuritynews.com/magento-backdoor-injection/

Apache HTTP Server Flaw Let Attackers Inject Malicious Headers & HTTP/2 DoS

Apache released updates to address several vulnerabilities impacting the Apache HTTP server that let attackers launch HTTP/2 DoS attacks and insert malicious headers.

Server operations are being adversely affected by these vulnerabilities, which are proving to be a serious danger.

A new class of vulnerabilities in various HTTP/2 protocol implementations is called CONTINUATION Flood. The primary cause of the denial of service is improper handling of HEADERS and several CONTINUATION frames.

In this case, a single TCP connection or a small number of frames can seriously interfere with server operations, resulting in crashes or severe performance declines.

Details Of The Vulnerabilities Addressed

CVE-2024-24795: HTTP Response Splitting In Multiple Modules

This is a low-severity vulnerability that enables an attacker to cause an HTTP desynchronization attack by injecting malicious response headers into backend applications using HTTP Response splitting across different modules in the Apache HTTP Server.

Jianjun Chen and Keran Mu from Tsinghua University and Zhongguancun Laboratory reported this issue.

This issue affects the Apache HTTP Server through 2.4.58.

Source : https://cybersecuritynews.com/apache-http-server-vulnerabilities/

Hackers Claiming XpressBees Data Leak: 95K User Personal Data Leaked

The logistics and supply chain company XpressBees has become the latest victim of a data breach.

A user by the alias "IntelBroker" on the notorious BreachForums community has claimed responsibility for the leak, which purportedly exposes the personal information of up to 95,000 users.

The IntelBroker posted a message on the forum stating that they had uploaded the XpressBees database for public download.

The post was accompanied by XpressBees' logo, a message of thanks for reading, and an invitation to enjoy the leaked data.

XpressBees' Data Compromise

XpressBees, known for its commitment to "delivering happiness," is now facing the grim reality of a cyber-attack that has jeopardized its customers' privacy.

The compromised data includes sensitive personal information that could be misused for identity theft, financial fraud, and other malicious activities.

While the specifics of the leaked data have not been fully disclosed, hackers commonly obtain names, addresses, email addresses, phone numbers, and sometimes even financial information like credit card details or bank account numbers in such breaches.

The extent of the damage is still being assessed, and XpressBees has yet to confirm the exact nature of the data accessed.

Source : https://cybersecuritynews.com/claiming-xpressbees-data-leak/

CYBER SECURITY NEWS

Cyber Attack Hits World’s Second Largest Lens-maker

HOYA CORPORATION, the world’s second-largest lens manufacturer, has reported an IT system incident that has disrupted its operations.

The Tokyo-based company, known for its advanced optics technology and a broad range of healthcare and imaging products, confirmed the cyber attack in a recent press release.

On the morning of March 30, 2024, an anomaly was detected in the IT systems at one of HOYA’s overseas offices.

The company immediately responded to the discovery of unauthorized access, isolating the compromised servers and notifying the relevant authorities in the affected countries.

HOYA has since enlisted the expertise of external forensic investigators to determine the cause and extent of the breach.

Impact on Operations

The cyber attack has had a tangible impact on HOYA’s business functions, with several production plants and product ordering systems experiencing disruptions. The company is actively working to mitigate the effects on its customers and resume normal operations.

HOYA’s commitment to customer service remains steadfast as it strives to fulfill customer demands and minimize inconvenience.

Source : https://cybersecuritynews.com/cyber-attack-hits-lens-maker/

New Fake E-Shopping Attack Hijacking Users Banking Credentials

A fake e-shop scam campaign has been targeting Southeast Asia since 2021, as CRIL observed a surge in activity in September 2022, with the campaign expanding from Malaysia to Vietnam and Myanmar.

The attackers use phishing websites to distribute a malicious APK (Android application package), which steals user credentials through SMS and can now also take screenshots and utilize accessibility services on the victim's device, giving the attackers more control.

Cybercriminals have launched a fake e-shop campaign in Malaysia since 2021 by impersonating cleaning services on social media, tricking victims into contacting them via WhatsApp.

It led users to download malicious APKs through phishing websites.

The malware specifically targeted login credentials for Malaysian banks, including Hong Leong, CIMB, Maybank, and others, demonstrating a growing trend of social engineering tactics combined with phishing attacks to steal banking information.

A fake e-shop campaign observed by Cyble has been expanding its operations across Southeast Asia, where attackers use phishing websites disguised as legitimate payment gateways to distribute malware.

Source : https://cybersecuritynews.com/fake-e-shopping-attack/

CYBER SECURITY NEWS

Google Pixel Phone Zero-days Exploited by Forensic Firms in the Wild : Patch Now

The Pixel Update Bulletin details security vulnerabilities and functional improvements for supported devices.

Updating to the April 2024 security patch level (2024-04-05 or later) addresses all these issues and those included in the April 2024 Android Security Bulletin.

The device's security patch level can be checked through the "Check and update your Android version" option. In contrast, Google strongly recommends installing this update on all supported Pixel devices to maintain security and improve functionality.

Google released an update addressing security vulnerabilities on Pixel devices. The update patches two critical vulnerabilities (CVE-2024-29745 and CVE-2024-29748) that might be under limited, targeted attacks.

CVE-2024-29745 is an information disclosure vulnerability in the bootloader. This program loads the operating system, while CVE-2024-29748 is a privilege escalation vulnerability in the Pixel firmware, potentially allowing attackers to gain more control over the device.

It is recommended that all Pixel users update their devices to the latest security patch (April 5, 2024, or later) to mitigate these vulnerabilities.

Source : https://cybersecuritynews.com/google-pixel-phone-zero-days-exploited-by-forensic-firms-in-the-wild-patch-now/

Rhadamanthys Stealer Using Weaponized PDF Files To Attack Oil And Gas Sector

Hackers use weaponized PDF files as they have the ability to incorporate malicious codes or scripts within a well-known and trusted form of PDF which is often not detected by security measures.

If the person opens one such malicious document, it may release malware payloads, steal sensitive data, or run random code on the infected device.

For hackers, these are useful ways into targeted systems as PDFs are common and everyday things. Cybersecurity researchers at Cofense recently discovered a malicious campaign in which Rhadamanthys stealer has been actively using weaponized PDF files to attack the oil and gas sector.

Rhadamanthys Stealer Via Weaponized PDF

The campaign mainly focused on the Oil & Gas sector but could change to other sectors.

It managed to achieve an alarming email delivery success by combining TTPs such as trusted domains, redirects, and clickable images to evade email security.

Rhadamanthys Stealer malware executable was used to download a malicious PDF during the infection chain.

Source : https://cybersecuritynews.com/rhadamanthys-stealer-weaponized-pdf-oil-gas-attack/

VMware SD-WAN Vulnerabilities Let Attackers Execute Arbitrary Commands

Multiple security flaws affecting VMware SD-WAN have been addressed, allowing arbitrary commands to be executed on the intended system.

If these vulnerabilities are successfully exploited, enterprises that use VMware SD-WAN to manage their network connections may be exposed to serious threats.

The vulnerabilities tracked as CVE-2024-22246, CVE-2024-22247, and CVE-2024-22248 impact VMware SD-WAN Edge and SD-WAN Orchestrator.

Unauthenticated Command Injection vulnerability – (CVE-2024-22246)

An unauthenticated command injection vulnerability in VMware SD-WAN Edge has the potential to cause remote code execution.

VMware determined that the issue has a maximum CVSSv3 base score of 7.4 and falls into the important severity level.

“A malicious actor with local access to the Edge Router UI during activation may be able to perform a command injection attack that could lead to full control of the router,” reads the security advisory released by VMware.

This security vulnerability was reported by Saif Aziz (@wr3nchsr) from CyShield.

Source : https://cybersecuritynews.com/vmware-sd-wan-vulnerabilities/

CYBER SECURITY NEWS

Chrome Zero-Day Vulnerability Exploited At Pwn2Own : Patch Now

Google fixed three vulnerabilities in the Chrome browser on Tuesday, along with another zero-day exploit that was exploited during the Pwn2Own Vancouver 2024 hacking contest.

Google recently fixed two more zero-day vulnerabilities that were exploited during the Pwn2Own hacking competition.

Palo Alto Networks' Edouard Bochin (@le_douds) and Tao Yan (@Ga1ois) reported the vulnerability identified as CVE-2024-3159 on March 22, 2024, during Pwn2Own 2024.

Both of them received $42,500 and 9 Master of Pwn points for successfully showcasing their attack against Microsoft Edge and Google Chrome.

Google has fixed the vulnerabilities in the Google Chrome Stable channel to 123.0.6312.105/.106/.107 for Windows and Mac and 123.0.6312.105 for Linux. The update will be rolled out in the upcoming days and weeks.

Specifics Of Zero-Day Flaw Addressed – CVE-2024-3159

The CVE-2024-3159 vulnerability is an out-of-bounds memory access in the V8 JavaScript engine.

By deceiving the victim into visiting a specially created HTML page, a remote attacker can exploit this vulnerability and obtain access to data that is beyond the memory buffer, so causing heap corruption.

Source : https://cybersecuritynews.com/chrome-zero-day-exploit-patch/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT

☎ +91 865 866 3664   www.qualysec.com   ✉ contact@qualysec.com