QUALYSEC
BEYOND CYBERSECURITY

2023

APRIL 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

New Google Chrome Zero-Day Bug Actively Exploited in Wide – Emergency Update!

Google released new security updates for actively exploited Chrome zero-day vulnerability that allows attackers to execute an arbitrary code to take complete control of the system remotely using the exploit in the Wild.

Google fixed its first and actively exploited zero-day this year, and it is a stable and extended channel update and released a new version, Chrome 112.0.5615.121, for Windows, Mac, and Linux.

In this update, Google issued a patch for 2 vulnerabilities, and the details remain undisclosed until most users get the patch.

CVE-2023-2033 is a Type Confusion in V8 vulnerability categorized as high severity. The vulnerability was reported by Clément Lecigne of Google's Threat Analysis Group on 2023-04-11, Clement already found the same type of vulnerability (CVE-2022-4262) last year, and the patch was issued in December.

"Google is aware that an exploit for CVE-2023-2033 exists in the wild," Google says.

A high-severity type Confusion vulnerability in the V8 Javascript engine affects all the Chrome versions that allow attackers to exploit the bug remotely by executing arbitrary code.

Source : https://cybersecuritynews.com/new-google-chrome-zero-bay-bug/

Pakistan Hackers Attack Indian Edu Sectors Using Weaponised Office Documents

SentinelLabs recently discovered a series of malicious Office files spreading the notorious Crimson RAT malware.

This RAT is notorious for being utilized by the notorious Transparent Tribe group (aka APT36), which has been actively targeting the educational sector in India.

This group has been active since at least 2013 and is suspected to be based in Pakistan. Apart from this, Transparent Tribe is not very sophisticated but highly persistent since it constantly adapts its operational strategy.

SentinelLabs has observed a shift in the focus of Transparent Tribe, which had previously concentrated its attacks on Indian military and government personnel.

However, it has been observed that they have extended their target in recent times to include educational institutions in the Indian subcontinent and students in these establishments.

Among the malware arsenals of the adversary used in the group's campaigns, Crimson RAT is a consistent staple.

Source : https://cybersecuritynews.com/pakistan-linked-hackers-target-indias-education-sector/

1M Times Downloaded Android Printing App Can Be Abused to Drop Malware

A critical security issue has been discovered by the Japanese Vulnerability Notes (JVN) with the Kyocera Android printing app.

The security flaw has been tracked as CVE-2023-25954. Specifically, the app is at risk of improper intent handling, which could enable malicious applications to exploit the flaw.

This would allow it to download harmful malware onto devices, posing a significant threat to users.

In light of the aforementioned security issue, KYOCERA has taken swift action and released a security bulletin to inform users of the potential vulnerability.

Products Affected

Here below, we have mentioned the products that are affected:-

- Android app “KYOCERA Mobile Print”, v3.2.0.230119, and earlier, it has 1 million downloads on Google Play.
- Android app “UTAX/TA MobilePrint”, v3.2.0.230119, and earlier, it has 100k downloads on Google Play.
- Android app “Olivetti Mobile Print”, v3.2.0.230119, and earlier, it has 10k downloads on Google Play.

Despite being published by different publishers, it has been discovered that all these three apps share the same source code.

Source : https://cybersecuritynews.com/android-printing-app/

iPhones Hacked via Zero-click Exploit to Drop QuaDream Spyware

In collaboration with Citizen Lab, Microsoft recently uncovered an alarming discovery about QuaDream, an Israel-based firm.

The company was found to be behind the development of commercial spyware dubbed “KingsPawn” that uses a zero-click exploit called “ENDOFDAYS” to compromise high-risk individuals’ iPhones.

Threat actors exploited a zero-day vulnerability that affected the iPhones running iOS 14 or later versions up to 14.4.2.

Between January 2021 and November 2021, the attack employed a sophisticated backdated technique involving “invisible iCloud calendar invitations,” making them nearly impossible to detect.

Zero-click Exploit to Drop Spyware

One way the ENDOFDAYS exploit could remain undetected by targets was by using backdated timestamps on iCloud calendar invitations.

When all these backdated invitations were sent to iOS users, they were automatically added to their calendars without the user having to do anything, reads Microsoft report.

This automatic addition provided a stealthy means for the exploit to run without the user’s knowledge.

Source : https://cybersecuritynews.com/iphones-zero-click-exploit/

Hackers Exploited Windows Zero-day For Ransomware Attacks

Microsoft recently fixed a zero-day vulnerability that threat actors exploited to gain unauthorized privileges in the Windows Common Log File System (CLFS).

The cybersecurity analysts at SecureList from Kaspersky affirmed that the threat actors reportedly used this exploit to deploy Nokoyawa ransomware payloads.
Microsoft has identified and assigned CVE-2023-28252 to a security vulnerability affecting the Common Log File System that could allow for unauthorized escalation of privileges.
While Microsoft taken swift action to address the issue and has released a patch on April 11, 2023, as part of its latest round of security updates known as “April Patch Tuesday.”

Here below, we have mentioned the name of those entities who have discovered this vulnerability:-

- Genwei Jiang of Mandiant
- Quan Jin of DBAPPSecurity’s WeBin Lab

Source : https://cybersecuritynews.com/hackers-windows-zero-day/

FBI has Warned People to Avoid Free Public Charging Ports

The FBI issued a warning on the evening of Maundy Thursday about using Free public charging ports. It stated that threat actors use public charging outlets in airports and coffee shops to inject malware and monitoring software.

As per the tweet on Twitter, the FBI said, “Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices.”

Two main types of “jacking” are done through public USB ports.

Juice Jacking

Juice jacking is a method in which threat actors steal account credentials, financial or any other sensitive information from devices while they are charged. This is done by loading malware onto the public charging stations that are triggered when a device is plugged in.

Video Jacking

Video Jacking is a method in which threat actors hide equipment in public charging stations to record activities on a device while plugged in. This ranges from entering a password to writing an email or accessing a banking application with a password.

Source : https://cybersecuritynews.com/free-public-charging-ports/

Microsoft Fixed A Windows 0-Day Along With 96 Other Vulnerabilities

Microsoft fixed a critical Elevation privilege zero-day vulnerability that affected the Windows Common Log File System Driver.

MS Office & Word RCE Bugs Fixed

Microsoft fixed the following remote code execution vulnerabilities that affect MS Office and Word.

CVE-2023-28285 – A Remote code execution vulnerability that affects MS Office allows an attacker to trick users into running malicious files from the local machine to exploit the vulnerability. Also, Microsoft clarifies that it doesn't mean arbitrary code, but the word Remote in the title refers to the attacker's location.

CVE-2023-28295 & CVE-2023-28287 – A Microsoft Publisher remote code execution vulnerability lets hackers gain system access by tricking the users into executing the malicious code that sends via email and downloaded from a malicious website.

CVE-2023-28311 – Microsoft Word Remote Code Execution Vulnerability allows attackers to trick users into running malicious files from the local machine to exploit the vulnerability.

You can refer here to the complete patch details for the full list of resolved vulnerabilities and advisories in the April 2023 Patch.

Source : https://cybersecuritynews.com/microsoft-fixed-a-windows-0-day-bug/

Hacker Group Selling Stolen Databases From Public Authorities

A threat actor group is known as “ARES” that deals in the selling of business and governmental authority databases has been detected by the CYFIRMA Research team.

The term “Ares” has previously been used to refer to the notorious Trojan malware “Ares Rootkit,” which was employed by hackers to hack into computers and steal sensitive data.

By actively seeking alliances with other threat actors and claiming connections with reputable hacker groups and ransomware operators, the investigation shows that ARES has exhibited behaviors compatible with “cartel-like behavior.”

Cybercriminal groups have accepted this affiliation. Late in 2021, this actor made his Telegram debut; since then, he has been linked to the RansomHouse ransomware operation, the KelvinSecurity data leak platform, and the Adrastea network access group.

ARES Group runs its website, including database leaks and a forum, which may compensate for the gap left by the now-defunct Breached forum.

Source : https://cybersecuritynews.com/hacker-selling-stolen-databases/

Latitude Financial Refuses Hackers' Ransom Demand in the Wake of Massive Data Breach

Latitude Financial has released a press release saying they will not be paying the ransom demand from the threat actors that infiltrated their network on 16 March 2023.

According to the release, "Latitude will not pay a ransom. This decision is consistent with the position of the Australian Government. We will not reward criminal behavior, nor do we believe that paying a ransom will result in the return or destruction of the stolen information.

"In line with advice from cybercrime experts, Latitude strongly believes that paying a ransom will be detrimental to our customers and cause harm to the broader community by encouraging further criminal attacks."

Further statements also indicated that they are working with the Australian Cyber Security Center and cyber-security experts to investigate the issue further.

As per the reports on 27 March 2023, the stolen data accounts for approximately 7.9 million License numbers of Australian and New Zealand drivers, of which nearly 40% (3.2 million) of them belonged to the data that the company got in the last ten years.

Source : https://cybersecuritynews.com/latitude-ransom-demand/

Balada Injector – Massive Ongoing WordPress Malware Infected Over 1 Million Websites

The campaign has been ongoing, using known vulnerabilities in themes and plugins to insert a malicious Linux backdoor.

While cybersecurity researchers have identified the backdoor as a "Balad Injector." It appears that the campaign in question has been actively running since 2017, with its primary objective being to redirect users to various types of online scams, and these include:-

- Fake tech support pages
- Lottery scams
- Push notification fraud

Long-running Infection Waves

Sucuri has recently identified the Balad Injector campaign as the same one Dr. Web reported in December 2022.

This campaign exploits the vulnerabilities in multiple plugins and themes to insert a backdoor, allowing attackers to gain unauthorized access to affected websites.

Sucuri has reported that the Balad Injector campaign operates in waves, with attacks occurring approximately once a month. To evade blocking lists and other security measures, the attackers use a freshly registered domain name for each wave of attacks.

Source : https://cybersecuritynews.com/wordpress-websites-infected/

KFC & Pizza Hut Discloses Data Breach – Users Personal Information Stolen

Yum! Brands, Inc., which runs the restaurants KFC, Pizza Hut, Taco Bell, and The Habit Burger Grill, submitted a notice of security breach to warn of a cybersecurity incident affecting individuals' personal information that happened in mid-January 2023.

Although some data had been taken from the company's network, the company had previously claimed no proof of identity theft or fraud involving individual users' data.

Insights of the Security Breach

Around January 13, 2023, Yum! Brands encountered a cybersecurity problem involving unauthorized access to some of their systems.

As soon as they learned about the issue, the company locked down the impacted systems, alerted federal law enforcement officials, and collaborated with top digital forensics and restoration teams to investigate and remediate the incident.

The company says it has implemented 24/7 detection and monitoring technologies. In addition, they involved experts in determining whether any individual's personal information might have been in the files impacted by the incident.

Source : https://cybersecuritynews.com/kfc-pizza-hut-breach/

New MITM Attack on Wi-Fi Networks Let Attackers Stealthily Hijack the Traffic

Recently, access to public Wi-Fi networks is easily feasible due to their availability in most common public places.

The nature of Wi-Fi networks is such that supplicants, or end hosts, can come from all corners of the world and be owned by individuals from diverse organizations.

This contrasts wired LANs like Ethernet, where the end hosts typically belong to the same organization.

With the rapid evolution of wireless networks, threat actors now have a greater opportunity to intercept other users' traffic in the same network.

That's why the security mechanisms for wireless networks are constantly evolving, from the outdated Wired Equivalent Privacy (WEP) to the latest standard of Wi-Fi Protected Access 3 (WPA3).

New MITM Attack

The open-access nature of public Wi-Fi networks makes them particularly vulnerable to MITM (Man-in-the-Middle) attacks.

In Evil Twins attacks, also known as "Rogue Access Point attacks," threat actors can deploy a fake wireless access point (AP) to intercept the traffic of unsuspecting victims.

Source : https://cybersecuritynews.com/mitm-attack-on-wi-fi-networks/

Hackers Injecting Code Into Headlight Wiring to Steal Cars

As technology advances, so do the methods of malicious individuals seeking to exploit it. A concerning trend in the automotive industry is the injection of code into the Electronic Control Unit (ECU) of vehicles, including the wiring for essential components such as headlights.

These subtle and stealthy actions grant hackers unauthorized access to keyless entry systems, putting vehicle owners at risk of theft and other crimes.

While this vulnerability has been tracked as “CVE-2023-29389” by the security experts, and this vulnerability is currently awaiting analysis.

Injecting Code Into Headlight Wiring

The discovery of a new Controller Area Network (CAN) injection attack technique was recently made by Ian Tabor in the automotive industry.

Ian Tabor’s investigation into the theft of his Toyota RAV4 led him to uncover this stealthy technique, which could potentially compromise the security of countless vehicles worldwide.

Source : https://cybersecuritynews.com/can-injectors/

“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