QUALYSEC
BEYOND CYBERSECURITY

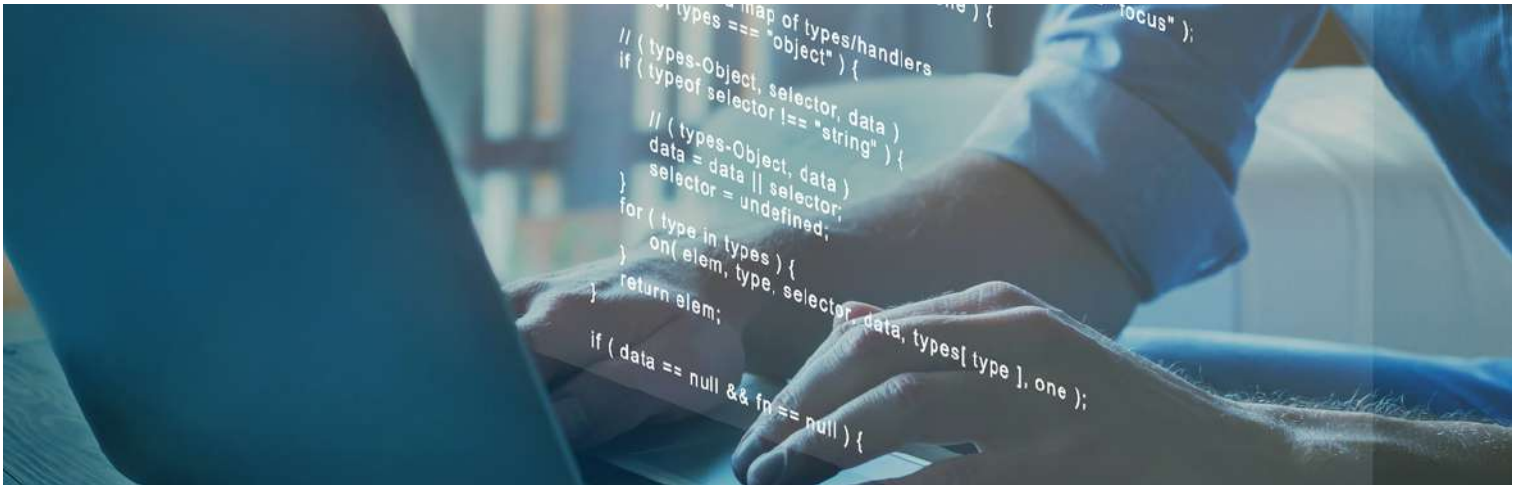
2024

JAN 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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



49 Unique Zero-days Uncovered in Pwn2Own Automotive

On the final day of Pwn2Own Automotive 2024 – Day 3, researchers were granted $1,323,750 in rewards for identifying 49 distinct zero-days. The first-ever Pwn2Own Automotive event has concluded! Synacktiv wins the Master of Pwn Trophy, earning 50 Master of Pwn Points and a $450,000 prize. Particularly, the infotainment system and modem of Tesla were attacked by the Synacktiv team, and each vulnerability earned $100,000.

Pwn2Own Day 3

Computest Sector 7 exploited the ChargePoint Home Flex by using a 2-bug chain. They get six Master of Pwn Points and $30,000.

The Sony XAV-AX5500 was compromised by Synacktiv. Together with four Master of Pwn Points, they receive $20,000.

Sina Kheirkhah exploited the Ubiquiti Connect EV by using a 2-bug chain. Six Master of Pwn Points and $30,000 are his earnings.

Connor Ford of Nettitude exploited the JuiceBox 40 Smart EV Charging Station by using a stack-based buffer overflow. Six Master of Pwn Points and $30,000 are his earnings. The EMPORIA EV Charger Level 2 was exploited by fuzzware.io via a buffer overflow. Six Master of Pwn Points and $60,000 are their earnings.

Source :https://cybersecuritynews.com/49-zero-days-pwn2own/

Cisco Unified Communications Flaw Let Attackers Execute Arbitrary Code

Cisco Unified Communications and Contact Center Solutions, known for their robustness, have recently been under scrutiny due to a critical vulnerability.

This flaw exposes an unsettling prospect: an unauthenticated, remote attacker gaining the ability to execute arbitrary code on affected devices. In this article, we dissect the intricacies of this security lapse.

The vulnerability CVE-2024-20253 stems from the improper processing of user-provided data, allowing attackers to exploit the system by sending a carefully crafted message to a listening port.

The consequence? The potential execution of arbitrary commands with the privileges of the web services user leads to an ominous scenario where the attacker could establish root access on the affected device.

The Affected Products and Exempted Solutions

The vulnerability affects several Cisco products, including Unified Communications Manager, IM & Presence Service, Session Management Edition, Contact Center Express, Unity Connection, and Virtualized Voice Browser.

Source : https://cybersecuritynews.com/cisco-unified-communications-flaw/

Critical Jenkins Vulnerability Let Attackers Execute Remote Code

Jenkins is an open-source automation server that is based on Java used for continuous integration and continuous delivery processes. Threat actors target Jenkins due to its widespread use in software development pipelines.

The widespread use of it provides an opportunity for threat actors to exploit vulnerabilities and gain unauthorized access to sensitive data, allowing them to potentially disrupt and compromise software development workflows.

Recently, the researchers' team at Jenkins uncovered a critical vulnerability that is tracked as "CVE-2024-23897," with a CVSS score of 9.8 in Jenkins that enables threat actors to execute remote code.

Flaw Profile

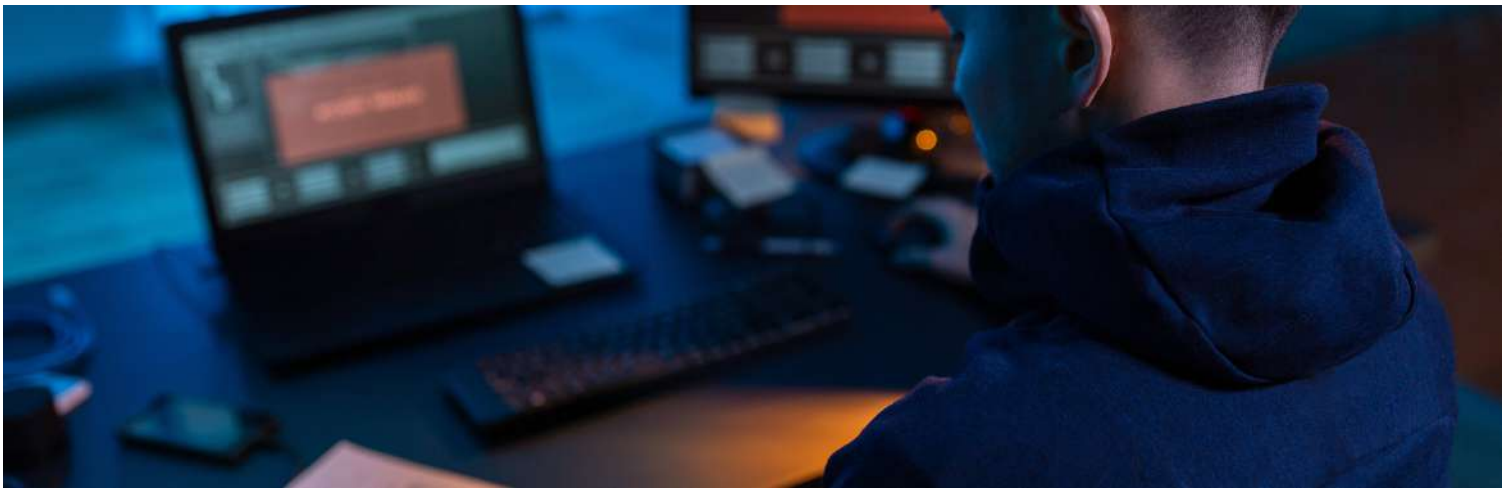
- CVE ID: CVE-2024-23897, CVSS score: 9.8, Severity: CRITICAL, Descriptions: Arbitrary file read vulnerability through the CLI can lead to RCE, SECURITY-3314

Critical Jenkins Vulnerability

Jenkins vulnerability arises from a default-enabled parser feature, 'expandAtFiles,' in CLI that impacts versions 2.441 and earlier.

Exploiting an arbitrary file reads the issue, and then the attackers can access the file system through the args4j library, which potentially compromises the system's security.

Source : https://cybersecuritynews.com/critical-jenkins-vulnerability/



The Invisible Threat: How Phishing Undermines Business Security

In an era where technology intertwines intricately with every facet of business operations, cybersecurity emerges as a buzzword and a cornerstone of organizational integrity.

But have you ever considered how vulnerable your business might be in the digital battlefield? One insidious player often slips through the cracks among many cyber threats—QR Code phishing. This deceptive practice, a staple in the arsenal of social engineering, has evolved into a formidable adversary against business security.

The Human Factor: A Cybersecurity Achilles' Heel

The age-old adage, "a chain is only as strong as its weakest link," finds profound relevance in cybersecurity. It is no revelation that the human element often bears this dubious distinction. The McAfee and Dell Technologies Global Small Business Study provides insight into this vulnerability. A staggering 73% of small businesses globally recognize cybersecurity as their most significant risk. Yet, despite this awareness, 44% of these businesses have tasted the bitter pill of a cyberattack.The fallout? A trifecta of dire consequences: compromised customer data (38%), lost passwords (34%), and the loss of other critical files (34%). This chilling reality begs a question – have we been underestimating the human factor in cybersecurity?

Source : https://cybersecuritynews.com/how-phishing-undermines-business-security/

Chrome Flaw Let Attacker Corrupt Memory via Crafted HTML Page

Google has updated the Stable channels to 121.0.6167.85 for Mac and Linux and 121.0.6167.85/.86 for Windows as part of a security update for Chrome.

There are 17 security fixes in this update. The upgrade will be rolled out over the coming few days and weeks.

High-Severity Flaws Addressed

A high-severity issue was identified as CVE-2024-0807, Use after free in WebAudio. This allowed a remote attacker to possibly exploit heap corruption via a crafted HTML page.

Google awarded a $11000 bounty after Huang Xilin of Ant Group Light-Year Security Lab reported it.

The vulnerability identified as Inappropriate implementation in accessibility (CVE-2024-0812) was determined to have a high severity.

This allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. Google announced a $9000 reward and stated the reporter was anonymous.

CVE-2024-0808, Integer underflow in WebUI, was found to be a high-severity issue. This enabled a remote attacker to potentially exploit heap corruption via a malicious file. A $6000 bounty was issued by Google, as reported by Lyra Rebane (rebane2001).

Source : https://cybersecuritynews.com/pure-malware-tools/

3000+ Discussions on Dark Web Posts to Use ChatGPT for Illegal Purposes

For the multitude of malicious activities, threat actors could exploit ChatGPT due to its conversational abilities, such as generating convincing phishing messages, crafting sophisticated social engineering attacks, and automating the production of misleading content.

Hackers can exploit the capacity of the model to understand and generate human-like text to trick users and automate fraudulent schemes, which makes it an attractive tool for them.

Kaspersky's Digital Footprint Intelligence service recently discovered more than 3000 discussions on Dark Web posts to use ChatGPT for illicit purposes.

Spike in Discussions Regarding the Illegal use of ChatGPT

Researchers noted a significant rise in Dark Web discussions on misusing ChatGPT. From January to December 2023, threat actors discussed using ChatGPT for illegal activities, like creating polymorphic malware to evade detection.

One suggestion involved using the OpenAI API to generate malicious code through a legitimate domain that poses a security threat. However, no such malware has been detected yet by security analysts, but it could emerge later.

Source : https://cybersecuritynews.com/3000-discussions-on-dark-web-posts/

5379 GitLab Servers are Vulnerable to Zero-Click Account Takeover Attacks

GitLab has released important security fixes for versions 16.7.2, 16.6.4, and 16.5.6 for GitLab Community Edition (CE) and Enterprise Edition (EE). The fixes include multiple bugs, including a critical account takeover vulnerability that does not require user interaction.

However, other fixes were approval and removal bypass from CODEOWNERS, execution of slash commands by abusing Slack/Mattermost integrations, new workspace creation under different root namespaces, and a commit signature validation ignore.

The CVEs for these vulnerabilities are CVE-2023-7028, CVE-2023-4812, CVE-2023-5356, CVE-2023-6955, and CVE-2023-2030. The severity for these vulnerabilities ranges between 3.5 (Low) to 10.0 (Critical).

Vulnerable GitLab Servers

CVE-2023-7028: Account Takeover

A threat actor can exploit this vulnerability and reroute the user account password reset email to an unverified email address, which could lead to a complete account takeover. Moreover, this can also be escalated to steal valuable information based on the permission of the compromised account.This vulnerability is said to be affecting GitLab CE/EE, affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2.

Source :https://cybersecuritynews.com/5379-gitlab-servers/

WhatsApp Privacy Flaw Devices Information to Any Other User

Hackers seek to exploit WhatsApp flaws to gain unauthorized access to user data, messages, and sensitive information.

Exploiting these flaws allows threat actors to compromise user privacy, conduct espionage, and engage in malicious activities.

Recently, a cybersecurity analyst, Tal Be'ery, discovered a WhatsApp privacy flaw that devices information on any other user

WhatsApp Privacy Flaw

For message confidentiality, WhatsApp, with over 5 billion downloads and 2.4 billion active users, relies on the End-to-End Encryption (E2EE) protocol.

WhatsApp introduced E2EE in 2016, where each app generates a unique crypto key for secure messaging. This key is tied to the device that changes during reinstallation to notify other users that a device switch has occurred.WhatsApp prevents information leaks during app reinstallation by maintaining the same key if restored from backup. In 2021, with multi-device architecture, companion devices generate their keys known as 'Identity keys,' valid until the app is uninstalled.

Source : https://cybersecuritynews.com/whatsapp-privacy-flaw/

Mass Exploitation of Ivanti VPN Exposes Corporate Networks to Hack Attacks

It was previously reported that Ivanti Connect Secure was vulnerable to an authentication bypass (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887) actively exploited by threat actors in the wild.

Moreover, these vulnerabilities were added to the CISA's known exploited vulnerability catalog, and all the FCEB agencies were informed to mitigate these vulnerabilities as soon as possible. However, there has been a massive exploitation of these vulnerabilities worldwide.

Massive Exploitation of Ivanti VPN

According to the reports shared with Cyber Security News, there were more than 26000 unique internet-facing Ivanti Connect Secure hosts. Among these, 412 hosts were found to be compromised by threat actors with a backdoor due to credential theft.

In addition to this, Ivanti has not yet released a patch to fix this vulnerability. Instead, they have provided recovery, workarounds, and mitigations for this vulnerability. As per the emergency directive released by CISA, the exploitation of these two vulnerabilities was mandated to be mitigated by Federal Civilian Executive Branch (FCEB) agencies.

Source : https://cybersecuritynews.com/mass-exploitation-of-ivanti-vpn/

Exploit Released for Critical GoAnywhere MFT Auth Bypass : Patch Now

Fortra-owned GoAnywhere MFT (Managed File Transfer) has been discovered with a new vulnerability that could allow an unauthorized threat actor to create an admin user via the administration panel. This vulnerability has been assigned with CVE-2024-0204, and the severity has been given as 9.8 (Critical).

However, Fortra has released a security advisory for addressing this vulnerability, which mentions that the affected products were Fortra GoAnywhere MFT 6.x from 6.0.1 and Fortra GoAnywhere MFT 7.x before 7.4.1. In addition, this vulnerability was identified as an authentication bypass vulnerability. GoAnywhere MFT Auth Bypass

According to the reports shared with Cyber Security News, researchers have been working on recreating this vulnerability, and a proof-of-concept has been published on GitHub.

As per Fortra's security advisory, the endpoint was stated as /InitialAccountSetup.xhtml, which can be deleted, and the service has to be restarted to mitigate the issue.

Further analyzing through the application directories, this endpoint was found to be mapped with the com.linoma.ga.ui.admin.users.InitialAccountSetupForm inside the GoAnywhere/adminroot/WEB-INF/forms-faces.xml file.

Source : https://cybersecuritynews.com/goanywhere-mft-bypass/

Atlassian Confluence Servers Attacked From 600+ IP Addresses

Atlassian disclosed a critical vulnerability last week related to Remote Code Execution (CVE-2023-22527). This particular vulnerability was reported to be affecting Confluence Data Center and Server versions released earlier than December 5, 2023.

Moreover, Atlassian also stated that the vulnerability was patched in the latest Confluence data center and server 8.5.4 (LTS) and 8.6.0 & 8.7.1 (Data Centers only). Moreover, version 8.5.4 also specified that it does not receive backported fixes due to the Security Bug fix policy.

CVE-2023-22527 allows an unauthenticated threat actor to execute remote commands on the affected installations. Moreover, this was a template injection vulnerability currently being exploited by threat actors. 600 Unique IPs

According to the reports shared with Cyber Security News, more than 600 IPs were observed attacking Atlassian Confluence with this vulnerability. Most of the attempts were attempts to do a callback with the “whoami” command execution.As for the originating IPs, most of them were traced back to Russia. Other commands used in the exploitation attempts were “id” and “cat /etc/shadow.” Atlassian urges all the users of Confluence servers to upgrade to the latest versions as soon as possible.

Source : https://cybersecuritynews.com/atlassian-servers600-ips/

Critical AI Security Flaws Let Attackers Bypass Detection & Execute Remote Code

Artificial Intelligence (AI) has become one of the fastest-booming technologies of this decade, with several advancements in multiple industries.

In several cases, threat actors have exploited AI systems to retrieve sensitive information later used in other attack vectors.

However, such a booming technology must be vigilant towards vulnerabilities that arise during the development or run time.

A bug bounty program was created to protect Artificial intelligence that detected several vulnerabilities using custom-developed and open-source tools.

Critical AI Security Flaws

According to the reports shared with Cyber Security News, there were more than 9 vulnerabilities detected this month. The most crucial ones were a Validation Bypass, Arbitrary File Overwrite via Malicious Source URL, and Local file inclusion.

The CVEs for these vulnerabilities were assigned as CVE-2024-0520 (10.0 – Critical), CVE-2023-6976 (8.8 – High), and CVE-2023-6977 (10.0 – Critical).

Source : https://cybersecuritynews.com/critical-ai-security-flaws/

“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