QUALYSEC
BEYOND CYBERSECURITY

2023
OCT 2ND WEEK
CYBER SECURITY NEWS

CONTACT US

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

Telegram, AWS, and Alibaba Cloud Users Targeted in Latest Supply Chain Attack

A new supply-chain attack, which was active throughout September 2023, has been discovered in which threat actors used Typosquatting and Startjacking techniques to lure developers using Alibaba cloud services, AWS, and Telegram into downloading malicious Pypi packages.

The threat actors, who had the name “kohlersbtuh15” uploaded a series of malicious packages into the open-source package manager Pypi in an attempt to perform a supply-chain attack on targeted victims, reads Checkmarx report.

Technical Analysis

Typosquatting is the technique in which a threat actor utilizes the human error of mistyping an installation command by publishing a similar package with the mistyped name. Additionally, if a developer searches for a box by mistyping the package name, they end up on the website of the malicious package.

Starjacking is a method in which a package hosted on a package manager is linked to a different unrelated package’s repository on GitHub. Both of these techniques are combined together to maximize the reach.

Source : https://cybersecuritynews.com/telegram-aws-alibaba-supply-chain-attack/

Microsoft Announced AI Bug Bounty Program that Rewards Up to $15,000

Microsoft created a new AI Bug Bounty program, which rewards people who help improve the AI Power Bing experience. The rewards range from $2,000 to $15,000.

The initial release of AI-powered Bing's scope product aims to provide enhanced security against emerging vulnerabilities. Through the integration of AI technology, Bing offers innovative experiences that directly impact the safety of our customers. The information has been reported by Microsoft.

You can get bounty awards for the following goods and integrations:

- AI-powered Bing experiences on bing.com in Browser (All significant vendors are supported, including Bing Chat, Bing Chat for Enterprise, and Bing Image Creator)
- AI-powered Bing integration in Microsoft Edge (Windows), including Bing Chat for Enterprise
- AI-powered Bing integration in the Microsoft Start Application (iOS and Android)
- AI-powered Bing integration in the Skype Mobile Application (iOS and Android)

Source : https://cybersecuritynews.com/microsoft-ai-bug-bounty-program/

Critical Google Chrome User-After-Free Site Isolation Flaw

As part of a security update for Chrome, Google has upgraded the Stable channels to 118.0.5993.70 for Mac and Linux and 118.0.5993.70/.71 for Windows.

The Extended Stable channel has been upgraded to 118.0.5993.71 for Windows and 118.0.5993.70 for Mac.

This release contains 20 security fixes. The upgrade will roll out over the following days and weeks.

Critical Vulnerability Addressed

A critical vulnerability identified as CVE-2023-5218, Use after free in Site Isolation. This was the issue reported on September 27, 2023.

Before 118.0.5993.70 in Google Chrome, use after free in Site Isolation flaw might have allowed a remote attacker to exploit heap corruption through a crafted HTML page.

Additionally, it requires some form of user involvement from the victim. Technical information is not known, and there is no publicly accessible exploit.

Medium Severity Vulnerabilities Addressed

Inappropriate implementation of Fullscreen is a bug of Medium severity listed as CVE-2023-5487. This was reported by Anonymous, who received a reward of $5000.

Source : https://cybersecuritynews.com/google-chrome-critical-flaw/

New WordPress Malware as Cache Plugin Creates Rogue Admin Account

A novel kind of malware that acts as a sophisticated backdoor that can carry out several operations while impersonating a legitimate plugin has been identified.

The malware has several features, including the ability to modify files, create an admin account, remotely activate and deactivate plugins, add filters to prevent itself from being listed among the activated plugins, and pinging functionality to check if the script is still active.

WordPress Malware as Cache Plugin

The malicious file has access to standard WordPress functionality just like other plugins since it operates as a plugin inside of the WordPress environment, reports Defiant, the company behind the WordPress security plugin Wordfence.

The code above shows the creation of a new user account with the username ‘superadmin’ and a hardcoded password with admin-level privileges. When it is no longer required, the next function is designed to delete the superadmin account.

Bot detection code is frequently seen in malware that presents average content to specific users while diverting them to malicious websites or presenting malicious content to other types of users.

Source : https://cybersecuritynews.com/wordpress-malware-as-cache-plugin/

Large-scale Akira Ransomware Attacking Unsecured Computers

In order to disrupt human-operated ransomware attacks and prevent attackers from advancing their objectives through lateral movement, it is crucial to swiftly contain any compromised user accounts.

Taking this step is essential to limit the attackers' ability to spread their malicious activity and protect the affected systems and data.

Lateral movement success relies on compromising user accounts and elevating permissions, often requiring access to high-level credentials in human-operated ransomware attacks.

Cybersecurity researchers at Microsoft recently identified a large-scale Akira ransomware operation attacking unsecured computers.

Akira Ransomware Attacking Unsecured Computers

Attackers use various methods, like credential dumping and keylogging, to compromise user accounts.

Neglecting credential security can lead to rapid domain admin-level account compromise, allowing attackers to take control of the network.

In some cases, it takes just one hop from the initial access point to compromise domain admin-level accounts.

An industrial engineering org faced a human-operated Akira ransomware attack in June 2023 that is linked to Storm-1567 by security analysts at Microsoft.

Source : https://cybersecuritynews.com/large-scale-akira-ransomware/

Google Initiates the End of Passwords, Making Passkeys the Default for Users

Google, a well-known tech giant, has introduced a new feature called “passwordless by default”. This feature aims to simplify the login process for users by eliminating the need for traditional passwords and instead relying on passkeys for authentication purposes.

In honor of Cybersecurity Awareness Month, a new and improved method for logging into online accounts has been introduced. This new system is both easier and more secure than previous methods, providing users with peace of mind and a streamlined experience.

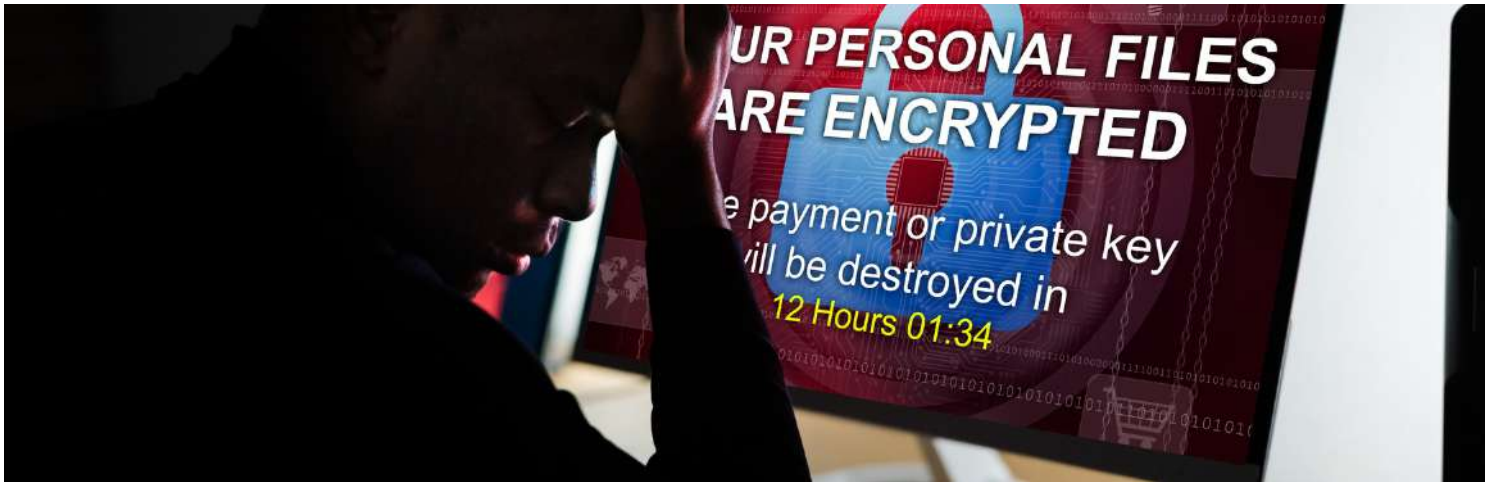
Passkeys by Default

A passkey is a unique and confidential identifier that establishes a secure connection between a user’s account and a website or application. With a passkey, users are able to access their accounts without the need to type in any login details, such as usernames or passwords, or undergo any other form of user verification process.

By logging into the account, you will be presented with convenient prompts that allow you to create and use passkeys for easier and quicker sign-ins in the future.

The statement refers to a setting in our Google Account that allows us to skip entering passwords whenever possible.

Source : https://cybersecuritynews.com/google-initiates-the-end-of-passwords/



Heap-based Buffer Overflow Flaw in cURL Library Using SOCKS5 Proxy

Previously, the maintainers of the popular curl command line tool posted a pre-announcement regarding two vulnerabilities that affected both the curl tool and the libcurl library.

However, the details of these vulnerabilities were not disclosed and were mentioned to be disclosed on October 11, 2023.

As per the post, the high-severity vulnerability under the CVE-2023-38545 was publicly disclosed by Curl. This vulnerability affects libcurl library from version 7.69.0 to 8.3.0.

Nevertheless, to exploit this vulnerability, an application must be configured to use SOCKS5 proxy modes and should attempt to resolve a hostname with inapplicable length.

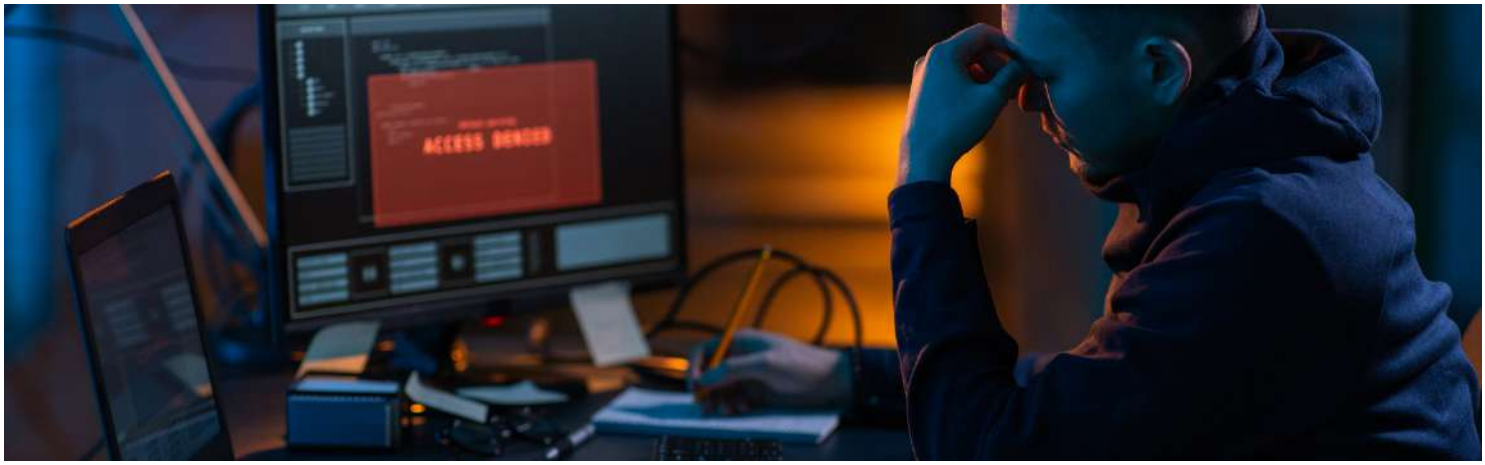
cURL Heap-based Buffer Overflow

This heap-based buffer overflow vulnerability exists when an application using a vulnerable version of curl or libcurl makes HTTP requests where a threat actor has enough privileges to set the “http_proxy” environment variable. The severity of this vulnerability is being analyzed.

There are prerequisites for an attacker before executing this attack. This includes

- The application must request socks5h.
- The application’s negotiation buffer is approximately smaller than 65k.
- The SOCKS server’s “hello” reply has a delay.

Source : https://cybersecuritynews.com/curl-heap-based-buffer-overflow-flaw/



How LLM-like Models like ChatGPT patch the Security Gaps in SoC Functions

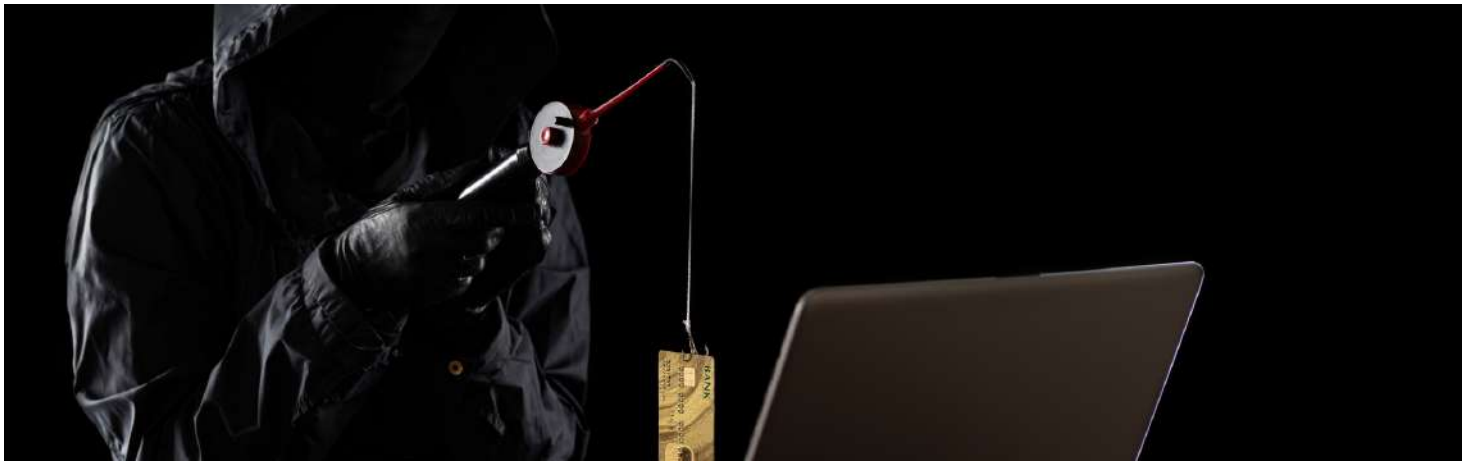
The emergence of Large Language Models (LLMs) is transforming NLP, enhancing performance across NLG, NLU, and information retrieval tasks.

They are primarily excellent in text-related tasks like generation, summarization, translation, and reasoning, demonstrating remarkable mastership.

A group of cybersecurity analysts (Dipayan Saha, Shams Tarek, Katayoon Yahyaei, Sujan Kumar Saha, Jingbo Zhou, Mark Tehranipoor, and Farimah Farahmandi) from the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA recently affirmed that LLM models like ChatGPT can patch the security gaps in SoC functions.

LLM-like Models - The growing prevalence of system-on-chip (SoC) technology in various devices raises security concerns due to complex interactions among integrated IP cores, making SoCs vulnerable to threats like information leakage and access control violations.The presence of third-party IPs, time-to-market pressures, and scalability issues challenge security verification for complex SoC designs. Current solutions struggle to keep up with evolving hardware threats and diverse designs.

Source : https://cybersecuritynews.com/how-llm-like-models-like-chatgpt/



Nation-state Hackers Exploiting Confluence Zero-day Vulnerability

Microsoft has detected the nation-state threat actor Storm-0062, also known as DarkShadow or Oro0lxy, exploiting CVE-2023-22515 in the wild since September 14, 2023.

The vulnerability was publicly disclosed on October 4, 2023, and this CVE-2023-22515 is a Confluence zero-day vulnerability.

Atlassian is investigating reports from a few customers regarding the potential exploitation of an undisclosed vulnerability in publicly accessible Confluence Data Center and Server instances, allowing unauthorized access and the creation of administrator accounts.

Here's what Atlassian stated:-"Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue."

Flaw profile

- CVE ID: CVE-2023-22515
- Description: Broken Access Control Vulnerability in Confluence Data Center and Server
- Advisory Release Date: Wed, Oct 4th, 2023 06:00 PDT
- Related Jira Ticket(s): CONFSERVER-92475
- Severity: Critical
- CVSS Score: 10.00

Source :https://cybersecuritynews.com/confluence-zero-day-vulnerability/

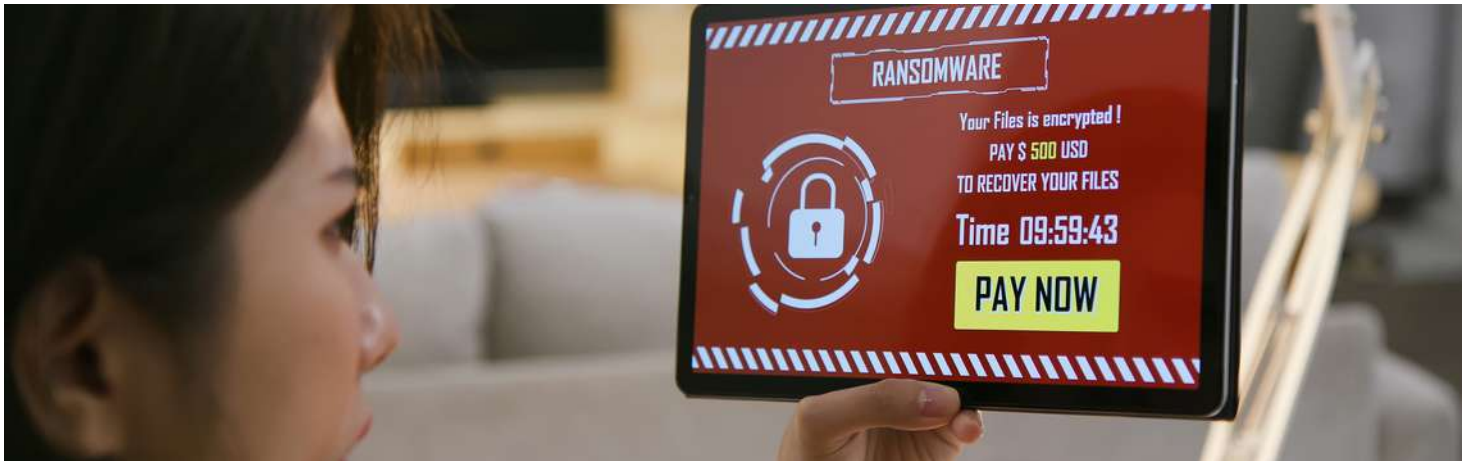
SAP Patches for XSS, Log Injection & Other Vulnerabilities

SAP has released the security patches for the Patch Day of October 2023, in which they release new Security Notes and 2 updates to the previously released Security Notes. There were 7 security vulnerabilities, including Cross-site scripting (XSS), Missing XML validation, Server-side Request Forgery, Missing Authorization check, Log injection, and Information disclosure vulnerabilities, that were fixed as part of the patch.

Vulnerabilities Discovered 1. **CVE-2023-42474**: Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Web Intelligence This vulnerability existed in the SAP BusinessObjects Web Intelligence due to a vulnerable URL parameter that could allow a threat actor to send a malicious link to a victim and extract sensitive information. The severity for this vulnerability was given as 6.8 (Medium).

2. **CVE-2023-40310**: Missing XML Validation vulnerability in SAP PowerDesigner Client (BPMN2 import)This vulnerability existed due to insufficient validation of BPMN2 XML documents imported from an untrusted source, resulting in URLs of external entities in the BPMN2 file being accessed. The severity for this vulnerability has been given as 6.5 (Medium).

Source : https://cybersecuritynews.com/sap-october-patches/



HTTP/2 Rapid Reset Zero-day Flaw Exploited to Launch Massive DDoS Attack

Cloudflare was unexpectedly hit by an enormous HTTP attack that peaked at over 201 million requests per second.

Starting on August 25, 2023, this onslaught posed a significant challenge, especially considering that it was initiated by a relatively modest botnet of just 20,000 machines.

To put this in perspective, the entire web typically handles between 1 to 3 billion requests per second. Detecting and mitigating these attacks required substantial efforts.

During the first wave of attacks, a small fraction of customer requests, approximately 1%, were initially affected.

However, Cloudflare's existing protection mechanisms were eventually refined to prevent the attacks from affecting its customers without causing harm to the company's systems.

Notably, these attacks were not exclusive to Cloudflare; other major industry players like Google and AWS experienced similar challenges.

HTTP/2 Rapid Reset Zero-day

To address this, Cloudflare collaborated with Google and AWS to coordinate the disclosure of the attack to affected vendors and critical infrastructure providers.

Source :https://cybersecuritynews.com/http-2-rapid-reset-zero-day/

“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