QUALYSEC
BEYOND CYBERSECURITY

2024

MAR 4TH WEEK

CYBER SECURITY NEWS

CONTACT US

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

Unsaflok Flaw Let Attackers Open Million of Doors in Seconds

Unsaflok, in Dormakaba's Saflok electronic RFID locks used in hotels and multi-family housing, allows attackers to forge a master keycard by exploiting weaknesses in the system and then using it to unlock any door within the affected property.

The vulnerability impacts over 3 million locks across 13,000 locations globally. All Saflok models, including the Saflok MT, Quantum Series, RT Series, Saffire Series, and Confidant Series, are susceptible if they are managed by System 6000 or Ambiance software.

While the lock model can be visually identified, there is no way to determine if a specific lock has been patched.

Researchers Lennert Wouters, Ian Carroll, rqu, BusesCanFly, Sam Curry, sshell, and Will Caruana disclosed a critical vulnerability (Unsaflok) in Dormakaba's Saflok electronic locks used in hotels and multi-family housing and by exploiting weaknesses in the system, attackers can forge a single keycard pair to unlock all doors within a facility.

More than 3 million locks across 13,000 properties in 131 countries are impacted, including Saflok MT, Quantum Series, RT Series, Saffire Series, and Confidant Series, which typically use Dormakaba's System 6000 or Ambiance software for management.

Source : https://cybersecuritynews.com/unsaflok-flaw/

Air Europa Announces Potential Compromise of Customer Data

Air Europa, a prominent Spanish airline, has announced a potential compromise of its customers' data following a security incident detected in October of the previous year.

This incident has raised alarms over the safety of personal information in the aviation sector, prompting a swift response from the company and its stakeholders.

Data Breach Details

The breach was first detected in October, and subsequent investigations by Air Europa have revealed that a significant amount of personal customer data may have been exposed.

According to an email sent to its customers, Reuters later saw that the compromised data included sensitive information such as names, ID card or passport details, dates of birth, telephone numbers, email addresses, and nationalities.

This incident marks a significant concern for Air Europa customers, as malicious entities could potentially misuse the leaked information.

Source : https://cybersecuritynews.com/air-europa-compromise-of-customer-data/

CISA & FBI Released Guide to Respond for DDoS Attacks

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation (FBI) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), has released a comprehensive guide.

It aimed at assisting federal, state, local, tribal, and territorial government entities in responding to Distributed Denial-of-Service (DDoS) attacks.

Understanding the Threat Landscape

DDoS attacks originate from multiple sources and can be particularly challenging to trace and block.

The guide provides an in-depth overview of the DoS and DDoS landscapes, detailing attack types, motivations, and potential impacts on government operations.

It emphasizes the importance of planning for emerging DDoS trends and technologies to better defend against malicious activity.

CISA and FBI have recently released a comprehensive guide that provides technical details and best practices to respond effectively to Distributed Denial of Service (DDoS) attacks.

.

Source : https://cybersecuritynews.com/cisa-fbi-released-guide-ddos-attacks/

AcidPour Attacking Linux Systems Running On x86 Architecture

Linux systems are used widely for servers, cloud environments, and IoT devices, which makes them an attractive target to cybercriminals, just as they are for any other platform.

Its extensive usage also provides a big area of attack, and its open-source characteristic enables hackers to analyze its codes for weak points.

Cybersecurity researchers at SentinelLabs recently discovered a new malware variant of AcidRain, dubbed “AcidPour,” that has been found attacking Linux systems running on x86 architecture.

AcidPour Attacking Linux Systems

On March 16th, 2024, a suspicious Linux binary uploaded from Ukraine was identified as a new variant called “AcidPour,” a wiper with similar and expanded capabilities to the infamous “AcidRain” that rendered KA-SAT modems inoperable during Russia’s invasion of Ukraine in 2022, disrupting services across Europe.

This is the first confirmed AcidRain variant detected since the original analysis which assessed medium-confidence developmental similarities between AcidRain and Russia’s VPNFilter malware.

Despite numerous cyber operations against Ukraine since 2022, no further AcidRain variants have been observed.

Source : https://cybersecuritynews.com/acidpour-attack-linux-x86/

167,500 Instances Found Vulnerable to Loop DoS Attack

A sweeping vulnerability has been uncovered, leaving an estimated 167,500 instances across various networks susceptible to a Loop Denial of Service (DoS) attack.

This discovery underscores the ever-present and evolving threats in the digital landscape, prompting an urgent call to action for organizations worldwide.

The Discovery

The vulnerability was first identified by Shadowserver, a renowned entity in the cybersecurity realm dedicated to identifying and mitigating cyber threats.

Through meticulous analysis and monitoring, Shadowserver's team stumbled upon a pattern of weakness in a staggering number of instances.

This flaw, if exploited, could allow attackers to initiate a Loop DoS attack, effectively crippling the targeted systems by overwhelming them with a flood of traffic.

According to a recent tweet from Shadowserver, there are over 167,500 instances that are vulnerable to the "Loop DoS" attack.

The vulnerability was discovered on March 20, 2024, and the affected IPs have been identified.

Source : https://cybersecuritynews.com/vulnerable-to-loop-dos-attack/

New Sysrv Botnet Abuses Google Subdomain To Spread XMRig Miner

First identified in 2020, Sysrv is a botnet that uses a Golang worm to infect devices and deploy cryptominers, propagates by exploiting network vulnerabilities, and has been continuously updated with new techniques by its operators.

Researchers have documented these advancements and explored the latest variant, including its infection chain, new methods, and Indicators of Compromise (IoCs).

Imperva Threat Research identified a botnet in early March based on blocked HTTP requests hitting their proxies, which exhibited characteristics of bot traffic, targeting a large number of websites across multiple countries.

The requests shared similar identifiers and aimed to leverage known security vulnerabilities in Apache Struts (CVE-2017-9805) and Atlassian Confluence (CVE-2023-22527 and CVE-2021-26084).

The analyzed dropper script, “ldr.sh,” resembles past Sysrv botnet iterations by defining variables for the compromised site URL (“cc”) and a random string (“sys”) based on the date’s MD5 hash.

A “get” function downloads files from provided URLs and is later used to download and run the second-stage malware from the compromised site.

Source :https://cybersecuritynews.com/sysrv-botnet-google-xmrig-spreader/

Polycab IT Infrastructure Targeted in Ransomware Attack

Threat actors often target GitHub users due to the plenty of valuable code repositories and sensitive information stored on the platform.

However, the collaborative nature of GitHub makes it an exceptional target for surveillance by threat actors seeking to gather intelligence on organizations and their development practices.

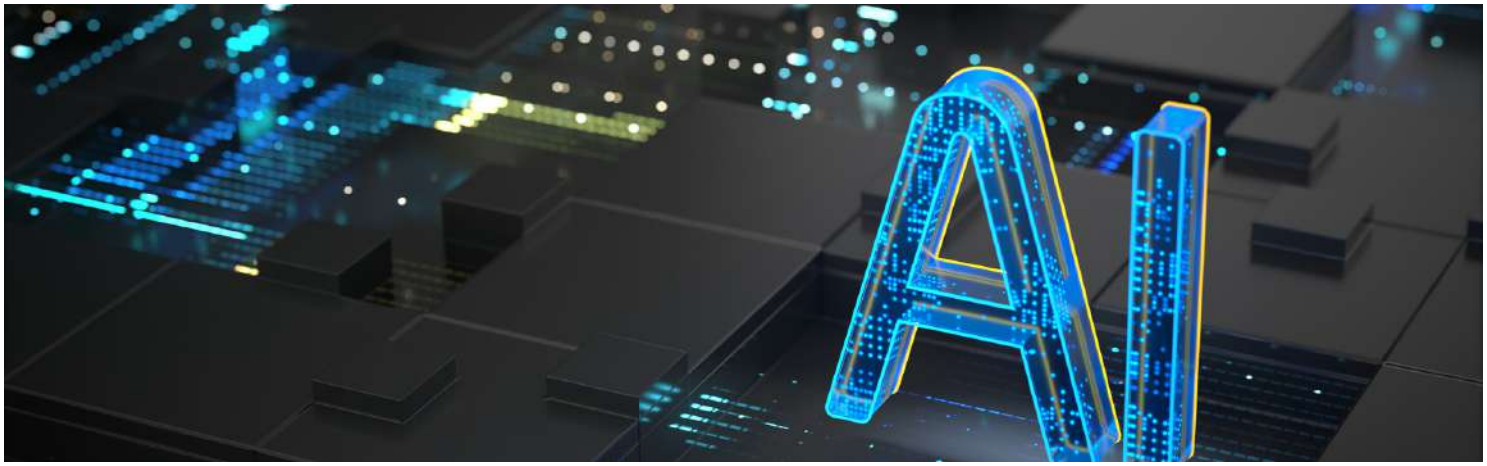
Cybersecurity analysts at G Data Defense recently discovered that threat actors are actively attacking GitHub users to steal login credentials via the Gitgub campaign.

Gitgub Campaign Attacking GitHub Users

RisePro employs encrypted strings and bloated installers crashing reverse-engineering tools. “Gitgub” exfiltrated over 700 data archives to Telegram. 13 repos from this RisePro stealer campaign featured the README lures. While the fake green Unicode circles mimicked build statuses for recency illusion. Red and green circles usually indicate real build outcomes on GitHub.The following download link remains the same across repos:- hxxps://site/INSTALLER%20PASSWORD.rar The user unpacks nested archives with “GIT1HUB1FREE” password. While the Installer_Mega_v0.7.4t.msi is the first executable.

Orca shows it unpacks the next stage using the “LBjWCsXKUz1Gwhg” password, and the final payload is “Installer-Ultimate_v4.3e.9b.exe.

Source : https://cybersecuritynews.com/polycab-it-infrastructure-targeted/



How ChatGPT and Bard Are Patching Up JavaScript Flaws : New Research

Despite JavaScript's widespread use, writing secure code remains challenging, leading to web application vulnerabilities.

Experiments on real-world vulnerabilities show LLMs hold promise for automated JavaScript program repair, but achieving correct fixes frequently requires providing an appropriate amount of contextual information in the prompt given to the LLM.

The following cybersecurity researchers from Simon Fraser University recently unveiled how ChatGPT and Bard are patching up the JavaScript flaws:–

- Tan Khang Le
- Saba Alimadadi
- Steven Y. Ko

Patching Up JavaScript FlawsDespite the use of techniques like static analysis and fuzzing, it is still sometimes difficult to understand and analyze programs because of the dynamic, asynchronous nature of JavaScript.

During the development process, many programmers create vulnerabilities without even knowing them as they try to make their programs secure.

Source : https://cybersecuritynews.com/chatgpt-bard-patching-up/

Atlassian Patches Critical Bamboo Server & Other 24 Flaws

A critical Bamboo Data Center and Server vulnerability has been discovered with a critical vulnerability which has been given CVE-2024-1597 and the severity was given as 10.0 (Critical).

This particular vulnerability was specifically mentioned by Atlassian that it is a non-atlassian Bamboo dependency.

“Atlassian’s application of the dependency presents a lower assessed risk, which is why we are disclosing this vulnerability in our monthly Security Bulletin instead of a Critical Security Advisory. ” reads the security bulletin from Atlassian.

Alongside of this, there were 24 other vulnerabilities that were fixed by Atlassian in several other products such as Bitbucket Data center and server, Confluence data center and server and Jira Software Data center and server.

The fixed vulnerabilities were related to several flaws including Denial of Service, Path Traversal, Remote Code execution and Server-side Request Forgery.

Source : https://cybersecuritynews.com/atlassian-patches-critical-bamboo-server-other-24-flaws/

Hackers Exploit DHCP To Escalate Privileges In Windows Domains

Researchers at Akamai have unveiled a new technique that could potentially put millions of Windows domains at risk.

This technique exploits the Dynamic Host Configuration Protocol (DHCP) administrators group to escalate privileges within Active Directory (AD) environments, a cornerstone of network management in numerous organizations worldwide.

The DHCP server, a critical component in network management, is responsible for assigning IP addresses to devices on a network.

However, when this server role is installed on a Domain Controller (DC), it opens up a Pandora's box. Researchers have found that this configuration can be manipulated to grant attackers domain admin privileges, essentially handing them the keys to the kingdom.

Microsoft DHCP Servers

This technique does not exploit a vulnerability in the traditional sense but abuses legitimate features, making it a particularly insidious threat.

With Microsoft DHCP servers running in approximately 40% of the networks monitored by Akamai, the potential impact is vast.

Beyond privilege escalation, the technique can also be used to create a stealthy domain persistence mechanism.

Source : https://cybersecuritynews.com/dhcp-exploit-privilege-escalation-windows/

“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