






2024

April 4th week

CYBER SECURITY NEWS

CONTACT US

-  www.qualysec.com
-  +91 865 866 3664
-  contact@qualysec.com



ICICI Bank Data Leak Exposes 17,000 Customers' Credit Card Data

ICICI Bank, one of India's leading private banks, has confirmed the exposure of sensitive credit card information belonging to thousands of customers.

The Mumbai-based bank acknowledged that a technical glitch in its mobile banking application, iMobile Pay, led to approximately 17,000 new credit cards being "erroneously mapped" to the wrong users.

The issue was first brought to light by customers who noticed unfamiliar credit card details within the app.

These details included the full credit card number, expiration date, and the card verification value (CVV), which are critical pieces of information for conducting financial transactions.

The breach was severe enough to allow users to view and potentially adjust settings for these cards, such as enabling foreign transactions or changing spending limits.

The bank's spokesperson stated, "The affected cards represent about 0.1% of ICICI Bank's credit card portfolio. In response to the incident, ICICI Bank has taken immediate action by blocking the impacted credit cards and has begun issuing new ones to the affected customers".



Cactus Ransomware Exploiting Qlik Servers Vulnerability

The Cactus ransomware gang has been exploiting vulnerable Qlik sense servers ever since November 2023 using multiple vulnerabilities such as [CVE-2023-41266](#) (Path Traversal), [CVE-2023-41265](#) (HTTP request Tunneling) and [CVE-2023-48365](#) (Unauthenticated Remote Code Execution).

Though Qlik has addressed these vulnerabilities with multiple security advisories, thousands of servers remain vulnerable to exploitation.

QlikSense is a data visualization and business intelligence tool that can help businesses perform data analysis and other operations.

Technical Analysis

Statistical Threat Reports

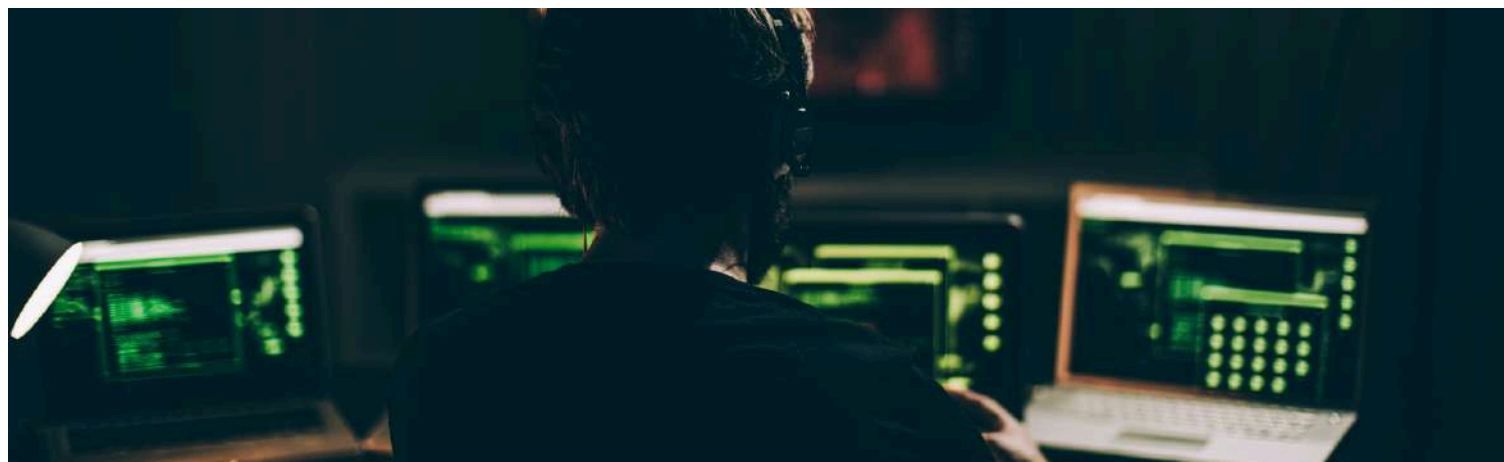
According to reports from Cyber Security News, threat actors were targeting these QlikSense servers with software vulnerabilities and misleading victims with cooked-up stories.

Nevertheless, the reports from Shadowserver indicate that there are 5,200+ internet-exposed Qlik servers, among which 3,100+ are vulnerable to exploitation by the Cactus group.

241 systems were discovered in the Netherlands alone, and the threat actors have already compromised 6 of them.

Identifying the list of servers and compromised servers involved multiple research steps.

Source : <https://cybersecuritynews.com/cactus-ransomware-qlik-server-exploit/>



Hackers Abuse Autodesk Drive For Hosting Weaponized PDF Files

Autodesk Drive is a data-sharing platform for organizations to share documents and files in the cloud.

It also supports 2D and 3D data files, including PDF files, which are free to use when other Autodesk products are subscribed.

However, a new attack campaign has been discovered.

This campaign abuses this Autodesk hosting platform to host malicious PDF files, which leads to phishing attacks on victims.

This phishing attack is aimed explicitly at harvesting Microsoft login credentials.

Technical Analysis

According to the reports shared with Cyber Security News, threat actors have been using compromised email accounts to find and target new victims.

Using compromised email accounts makes it less suspicious for users to visit the embedded Autodesk links.

The emails sent by the threat actors from these compromised accounts also include the legitimate email signature footer.

When victims click on the Autodesk drive links on these emails, they are taken to the links to view the PDF document, which mainly contains the sender's name and the company they work for to add trust to the phishing attack.



MuddyWater Hackers Abusing Legitimate RMM Tool to Deliver Malware

The Iranian state-sponsored threat actor MuddyWater has been observed exploiting a legitimate remote monitoring and management (RMM) tool, Atera Agent, to conduct a sophisticated malware delivery campaign.

This alarming trend has been under scrutiny since the beginning of 2024, with a notable increase in activity since October 2023, coinciding with the Hamas attack during the same period.

MuddyWater, recognized for its state-sponsored cyber activities, has a history of leveraging legitimate RMM software to deploy initial payloads in its cyberattacks.

This tactic has been a part of their modus operandi since at least 2021.

According to the Harfang Lab report, the group's strategic use of RMM tools allows it to maintain a low profile, making its malicious activities more complicated to detect as they blend in with regular network traffic.

MuddyWater Hackers

The MuddyWater group, also known as SeedWorm or TEMP.Zagros, has been active since 2017 and is known for its espionage campaigns that primarily target entities in the Middle East.

However, their activities have expanded globally, affecting various sectors, including telecommunications, government, and oil industries.

The group's sophisticated techniques and state backing make them a formidable threat in the cyber domain.

Source : <https://cybersecuritynews.com/muddywater-hackers-abusing-rmm-tool-deliver-malware/>



Hackers Actively Exploiting WP Automatic Updates Plugin Vulnerability

Hackers often target WordPress plugins as they have security loopholes that they can exploit to hack into sites without permission.

Once they have found them, threat actors can insert corrupted scripts into these loopholes to compromise the system, obtain secret data, and carry out any other attack that serves their requirements.

Cybersecurity researchers at WPScan recently discovered that hackers have been actively exploiting the WP Automatic updates plugin vulnerability, tracked as "CVE-2024-27956."

Flaw Profile

- CVE ID: CVE-2024-27956
- WP-Automatic Vulnerable Versions: < 3.9.2.0
- CVSSv3.1: 9.8
- CVSS severity: High
- Fixed in: 3.92.1
- Classification: SQL Injection
- Patch priority: High

WP Automatic Updates Under Attack

This critical flaw in the WP-Automatic plugin allows threat actors to bypass authentication, create admin accounts, upload malicious files, and potentially compromise affected websites through a SQL injection vulnerability that was discovered a few weeks ago.

Source : <https://cybersecuritynews.com/hackers-wp-automatic-vulnerability/>



Microsoft Releases Historical MS-DOS 4.0 Source Code to the Public

In a significant move for tech enthusiasts and historians alike, Microsoft has made the source code for MS-DOS 4.0 publicly available.

This decision marks a pivotal moment in the accessibility of historical software, allowing developers, students, and technology aficionados to explore the inner workings of one of the most influential operating systems in the history of personal computing.

Microsoft provided the source code for MS-DOS versions 1.25 and 2.0 to the Computer History Museum ten years ago., which was later republished for reference. This operating system's 8086 assembly code, written over 45 years ago, is remarkable.

"Today, IBM and we are releasing MS-DOS 4.00's source code under the MIT license in the spirit of open innovation. MS worked with IBM for parts of DOS 4.0 and created Multitasking DOS, which was never widely released," Microsoft said.

Background on MS-DOS

Microsoft Disk Operating System, commonly known as MS-DOS, was the dominant operating system for personal computers compatible with IBM PCs during the 1980s and early 1990s.

Initially developed in 1981, MS-DOS was critical in the personal computing revolution. It provided a command line interface for users to execute programs and manage files.

Source : <https://cybersecuritynews.com/microsoft-releases-ms-dos-4-0-source-code/>



PoC Exploit Released For Critical Flowmon Vulnerability

Progress addressed a critical vulnerability last week, which was associated with an unauthenticated Command injection on the Progress Flowmon product.

This vulnerability was assigned [CVE-2024-2189](#), and the severity was given as 10.0 (Critical).

Progress Flowmon is a network monitoring and analysis tool that gathers insights about network traffic, performance, and security. Its Web application uses a Nette PHP framework.

However, Progress released a security advisory for patching this vulnerability, urging all users to patch them accordingly.

To explain the vulnerability and exploitation further, a proof-of-concept for this vulnerability has been published.

Critical Flowmon Vulnerability

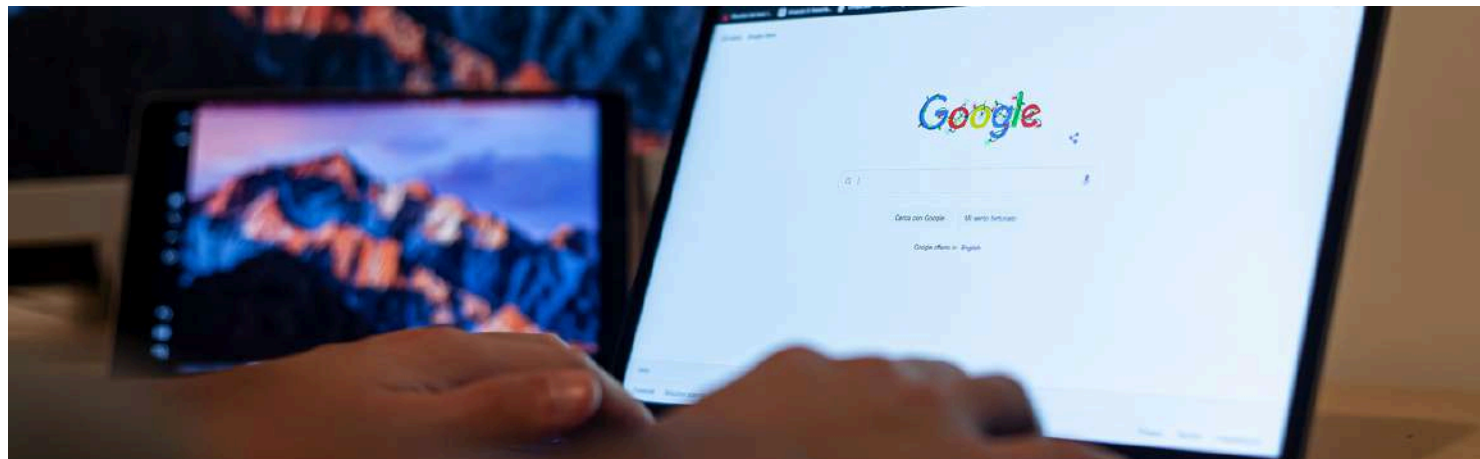
The researchers enumerated unauthenticated endpoints specified in the "AllowedModulesDecider.php" file, which consisted of an array named "ALLOWED_TO_UNLOGGED_USERS."

This array defines the modules of Flowmon that are accessible without authentication.

Further analyzing the code of the allowed list modules identified a specific code for generating PDFs under the name "Service:Pdf:Confluence."

The path for this module in the Nette Framework was "/service.pdfs/confluence"

Source : <https://cybersecuritynews.com/poc-exploit-critical-flowmon-vulnerability/>



Chrome Critical Flaw Let Attackers Execute Arbitrary Code : Patch Now

Google announced the release of Chrome 124, which fixes four vulnerabilities, including a critical security issue that allows attackers to execute arbitrary code.

Over the next few days or weeks, the Google Stable channel will be updated to 124.0.6367.78/.79 for Windows and Mac and 124.0.6367.78 for Linux.

Google said the Extended Stable channel has been updated to 124.0.6367.78/.79 for Mac and Windows and will be available over the next few days and weeks.

Critical Vulnerability Addressed

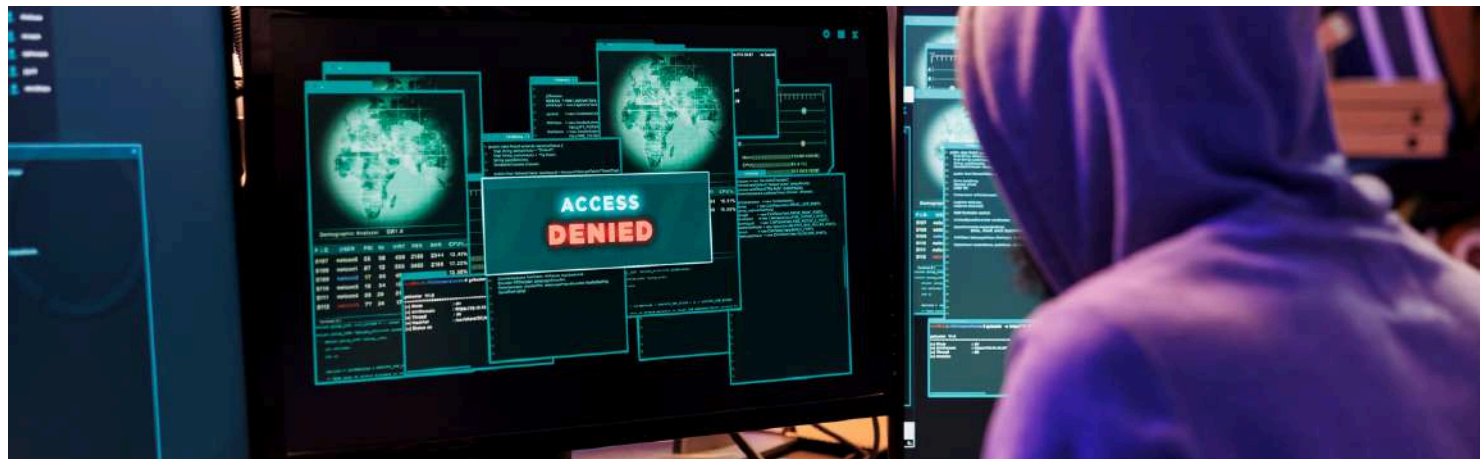
A critical security vulnerability is CVE-2024-4058, Type Confusion in ANGLE graphics layer engine.

This vulnerability can be used remotely to execute arbitrary code or do limited user interaction sandbox escapes.

Typically, arbitrary code execution allows the attacker to enter a system without authorization or carry out operations beyond the authors' intentions, which may result in data loss, corruption, or system compromise.

Google awarded a \$16000 bounty after Toan (suto) Pham and Bao (zx) Pham of Qrious Secure reported this critical security flaw.

Source : <https://cybersecuritynews.com/chrome-critical-security-update/>



Hackers Exploit Google Ads to Spread IP Scanner with Concealed Backdoor

Malicious actors are distributing a new backdoor, MadMxShell, through a Google Ads campaign that impersonates an IP scanner. This Windows backdoor leverages DNS MX queries for communication with its command-and-control server.

The technique involves encoding data within subdomains of DNS MX queries to send information to the attacker and receiving commands encoded within the response packets.

MadMxShell allows the attacker to collect system data, execute commands through the command prompt, and manipulate files on the compromised machine.

Advertisers are using malvertising, placing malicious ads disguised as legitimate software, to spread a sophisticated Windows backdoor called MadMxShell for the first time, which highlights a new tactic for delivering advanced malware.

The attackers exploited Google Ads by registering domains imitating popular IP scanner software, tricking users into downloading the backdoor, bypassing traditional malware detection methods, and emphasizing the need for increased vigilance against malvertising.

An attacker leverages social engineering tactics to deceive a user searching for legitimate IP scanning tools, where the user is tricked into clicking on a malicious Google ad that directs them to a typosquatting domain mimicking a popular download site.

Upon clicking the download button on this fake site, a malicious ZIP archive disguised as a legitimate IP scanner ("Advanced-ip-scanner.zip") is downloaded.

Source : <https://cybersecuritynews.com/google-ads-to-spread-ip-scanner/>



Hackers Employ Black Hat SEO Techniques To Deliver Malware

Hackers use black hat SEO methods to manipulate search engine rankings and make malicious or fraudulent websites more visible.

Recently, Zscaler cybersecurity researchers have seen a wave of fraudulent sites hosted on well-known web hosting services and blogging platforms that threat actors use for SEO poisoning and malware distribution.

Using legitimate hosting platforms allows attackers to quickly carry out SEO poisoning attacks, artificially elevating the ranking of harmful content on search results pages.

The website below appears legitimate; however, it carries malware that deceives people into downloading malicious software using search results.

The adversaries create fake sites that go unnoticed by the hosting services.

Unknowingly, users are directed to malicious sites when they search and click on links. They likely skip direct URL access because it could be subjected to security analysis.

These sites check referral URLs, and if they come from search engines, they proceed. However, if there is direct access without any redirection, they should not proceed to evade researchers' detection.

Source : <https://cybersecuritynews.com/hackers-black-hat-seo-malware-delivery/>



Google Meet Now Allows Non-Google Account Users to Join Encrypted Calls

Google has announced that external participants without Google accounts can join client-side encrypted Google Meet calls.

This move marks a substantial step in balancing user accessibility with robust security measures.

Google Meet has become an essential tool for virtual meetings, especially with the rise of remote work and the need for secure communication channels.

Historically, access to certain security features, such as end-to-end encryption, was limited to users within the Google ecosystem.

However, as the need for cross-platform collaboration grows, Google has evolved its service to accommodate secure participation from users outside of its domain.

Significance and Impact

This update is particularly noteworthy for organizations that handle sensitive information and require stringent security protocols.

By enabling client-side encryption for external participants, Google Meet ensures that all parties in a call can communicate securely, regardless of their email domain.

This level of security was previously unavailable to non-Google account holders, potentially limiting the platform's use in specific professional contexts.

Source : <https://cybersecuritynews.com/google-meet-encrypted-calls/>



“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