






**2024**

**May 1st week**

# **CYBER SECURITY NEWS**

## **CONTACT US**

-  [www.qualysec.com](http://www.qualysec.com)
-  +91 865 866 3664
-  [contact@qualysec.com](mailto:contact@qualysec.com)



## **CISA Warns Of Hackers Actively Attacking GitLab Password Reset Vulnerability**

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a critical alert concerning a newly identified vulnerability in GitLab, a widely used cloud-based, open-source Git repository platform.

The vulnerability cataloged as CVE-2023-7028, involves improper access control mechanisms in both the Community and Enterprise editions of GitLab.

Cybercriminals exploit this flaw to bypass password reset protocols, posing a significant threat to thousands of organizations globally.

GitLab is integral to the operations of over 38,000 companies worldwide, serving as a crucial tool for software development, continuous integration, and continuous deployment (CI/CD) processes.

Exploiting CVE-2023-7028 allows attackers to gain unauthorized access to private projects and sensitive data, leading to potential intellectual property theft and operational disruption.

This vulnerability compromises the security of the affected systems and threatens the integrity of the software development and deployment pipeline, which can have cascading effects on the reliability and security of applications being developed using GitLab.



## NCSC Warns of Russian Hackers Attacking Critical National Infrastructure

The National Cyber Security Centre (NCSC) has issued a stark warning about a new wave of cyber threats from Russian-aligned groups targeting the UK's critical national infrastructure.

Over the past 18 months, these groups have evolved, showing a solid ideological alignment with Russia's geopolitical interests, particularly evident since the onset of Russia's invasion of Ukraine.

Unlike traditional state-controlled cyber espionage units, these groups operate with a degree of autonomy that makes their actions unpredictable and potentially more widespread.

Their primary motivation appears to be ideological rather than financial, aiming to disrupt and destabilize rather than seek monetary gain.

### Unpredictable and Broad Targeting

The NCSC's alert highlights the less constrained nature of these groups compared to more formal state-sponsored actors.

This autonomy allows them to cast a wider net in their cyber operations, which traditionally include Distributed Denial of Service (DDoS) attacks, website defacements, and the dissemination of misinformation.

However, there is a growing concern that their ambitions are escalating towards more destructive attacks, particularly against sectors deemed part of the critical national infrastructure such as energy, telecommunications, and transportation.

**Source :** <https://cybersecuritynews.com/ncsc-warns-russian-hackers/>



## **New macOS Adload Malware Bypasses Built-in macOS Antivirus Detection**

A new variant of the notorious Adload malware has been discovered to bypass the latest updates to Apple's built-in antivirus, XProtect.

Despite Apple's efforts to fortify its defenses with a significant update to its malware signature list, Adload's authors have swiftly adapted, rendering these new measures ineffective against the latest iterations of the malware.

### Apple's Massive Adload Signature Update

Apple's security team recently implemented a substantial update to XProtect, adding 74 new rules in version 2192 and 10 additional rules in version 2193, released on April 30th.

This update aimed to combat the Adload adware, which has been a persistent threat to macOS devices.

According to the recent report by SentinelOne, a new strain of Adload malware has been discovered that is capable of bypassing the built-in antivirus detection of macOS, posing a significant threat to the security of Mac systems.

Before this update, XProtect had 207 rules, of which a significant portion targeted historical versions of Adload.

The update marked a 24% increase in the rule count, showcasing Apple's commitment to combating this pervasive adware.



## **Beware! Threat Actors Selling RDP Access on Hacker Forums**

Cybersecurity communities are on high alert as threat actors have begun selling Remote Desktop Protocol (RDP) access on underground hacker forums.

This alarming trend poses significant risks to individual and organizational cybersecurity, potentially allowing unauthorized access to sensitive information and critical systems.

According to a recent tweet from Dark Web Informer, threat actors sell access to RDP (Remote Desktop Protocol) on hacker forums.

### The Mechanics of the Threat

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that allows users to connect to another computer over a network connection.

In the hands of legitimate users, RDP is a powerful tool for remote administration and support.

However, in the wrong hands, it can serve as a gateway for cybercriminals to install malware, steal confidential data, or gain control over critical infrastructure.

The sale of RDP access typically involves credentials that include IP addresses, usernames, and passwords of vulnerable or compromised systems. These credentials are often obtained through various means, such as phishing attacks, credential stuffing, or exploiting vulnerabilities in the RDP setup itself.

The availability of RDP access on hacker forums is not just a problem for the affected systems but poses a broader threat to cybersecurity.

**Source : <https://cybersecuritynews.com/beware-threat-actors/>**



## Critical MailCleaner Vulnerabilities Let Attackers Execute arbitrary command

Critical vulnerabilities in MailCleaner versions before 2023.03.14 allow remote attackers to take complete control of the appliance through malicious emails, administrator interaction with attacker sites or links, and exploitation of SOAP endpoints, which compromises the confidentiality and integrity of the MailCleaner system and any emails processed by it.

Additionally, authenticated attackers with administrative privileges can gain further control by executing arbitrary commands or manipulating files on the system, posing a significant risk, especially in cluster deployments where a single compromised machine can grant attackers control of all cluster members.

A critical vulnerability in MailCleaner's email cleaning cronjob allows remote attackers to gain root access through a crafted email, which exploits an OS command injection flaw, enabling arbitrary command execution and complete system compromise.

By taking control of the MailCleaner appliance, attackers can intercept and manipulate all emails the system processes.

An unauthenticated attacker can exploit a stored XSS vulnerability in the admin dashboard via a malicious email, which injects malicious JavaScript, allowing session hijacking, data theft, or unauthorized actions as an admin.

This XSS can be chained for OS command injection when combined with other vulnerabilities, significantly amplifying the attack potential.

**Source :** <https://cybersecuritynews.com/critical-mailcleaner-vulnerabilities/>



## **Dropbox Sign Hacked: Attackers Stolen API Keys, MFA, & Hashed Passwords**

Dropbox disclosed a significant security breach affecting its electronic signature service, Dropbox Sign (formerly known as HelloSign).

The incident, which came to light on April 24, involved unauthorized access to the Dropbox Sign production environment, exposing sensitive customer information.

Dropbox's security team was alerted to the breach on April 24 after detecting unauthorized access to the Dropbox Sign production environment.

A thorough investigation revealed that a threat actor had infiltrated the system and gained access to a wealth of customer data.

### **Security Breach**

The breach was traced back to a compromised service account within Dropbox Sign's backend, a critical component used for executing applications and running automated services. In response to the breach, Dropbox has taken swift action to mitigate the impact on its users.

The company's security measures included resetting passwords, logging users out of all connected devices, and initiating the rotation of all API keys and OAuth tokens.

These steps are part of Dropbox's broader effort to secure its systems and protect user data from further unauthorized access.



## Russian Hackers Exploit Outlook Flaw to Hijack Numerous Email Accounts

In a significant cybersecurity development, Russian state-sponsored hackers, identified as APT28 or Fancy Bear, have been exploiting a critical vulnerability in Microsoft Outlook to hijack email accounts on a large scale.

This group, linked to Russia's military intelligence agency GRU, has targeted government agencies, energy sectors, transportation systems, and other key organizations across the United States, Europe, and the Middle East.

The exploited vulnerability, tracked as [CVE-2023-23397](#), is a severe elevation of privilege flaw in Outlook on Windows.

Microsoft first patched it in March 2023, but the hackers have continued to leverage this and other vulnerabilities to conduct sophisticated cyber espionage operations.

The CVE-2023-23397 vulnerability allows attackers to send specially crafted messages that exploit the Outlook application to execute unauthorized commands.

This flaw enables the attackers to elevate their privileges within the system without requiring user interaction, facilitating unauthorized access to sensitive information and email accounts.





## Android Bug Leaks DNS Traffic to Hackers While Switching VPN Servers

Android's operating system has identified a critical vulnerability that allows DNS traffic to leak during VPN server switches, potentially exposing users' internet activity to cybercriminals.

The issue, which affects multiple versions of Android, including the latest Android 14, was first reported by a user on Reddit and subsequently confirmed by Mullvad VPN through an internal investigation. The vulnerability was uncovered when a user noticed DNS queries leaking while toggling a VPN connection on and off, despite having the "Block connections without VPN" setting enabled. Mullvad VPN's subsequent investigation revealed that this was not an isolated incident but part of a broader issue within the Android OS.

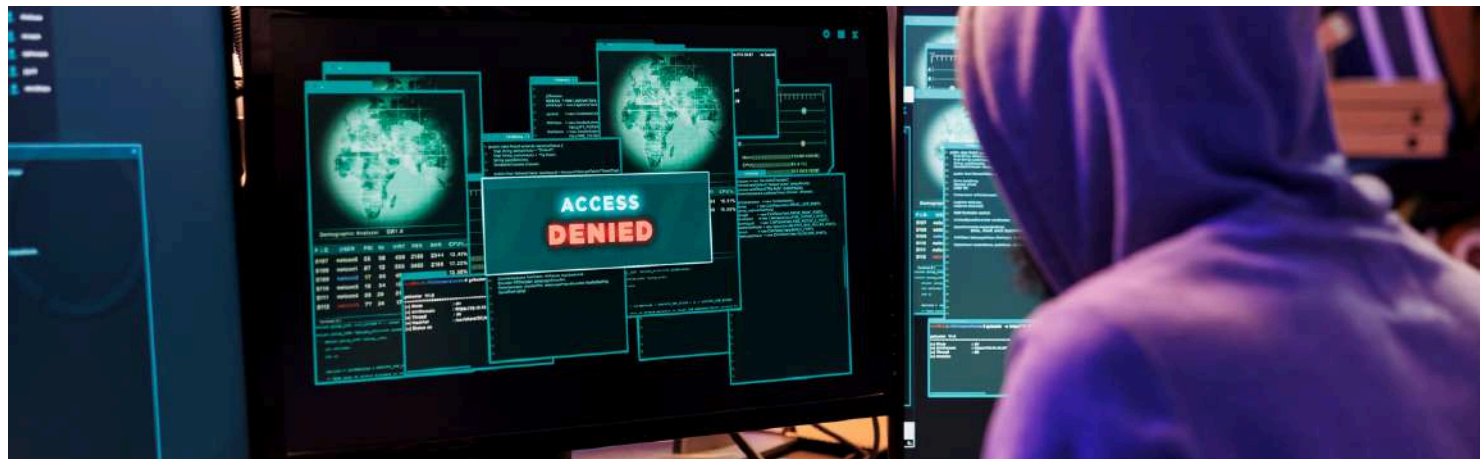
### Android Bug Leaks DNS Traffic

The DNS leaks occur under specific conditions:

- When a VPN is active, no DNS server is configured.
- During brief periods when a VPN app is reconfiguring the tunnel or if it crashes.

The leaks are primarily associated with direct calls to the C function `getaddrinfo`. Applications that resolve domain names using this method, such as the Chrome browser, are particularly susceptible to leaking DNS queries in the scenarios described.

Source : <https://cybersecuritynews.com/android-bug-leaks-dns-traffic/>



## ShadowSyndicate Hackers Exploit Aiohttp Vulnerability To Steal Sensitive Data

A directory traversal vulnerability ([CVE-2024-23334](#)) was identified in aiohttp versions before 3.9.2.

This vulnerability allows remote attackers to access sensitive files on the server because aiohttp doesn't validate file reading within the root directory when 'follow\_symlinks' is enabled.

Aiohttp is a popular asynchronous [HTTP framework](#) used in over 43,000 internet-exposed instances, making them prime targets for attackers, as patching to Aiohttp 3.9.2 or later is crucial to mitigate this vulnerability.

One of the most widely used Python libraries for asynchronous HTTP communication, it has a directory traversal vulnerability (CVE-2024-23334) that can be exploited by unauthenticated attackers.

The critical flaw (CVSS: 7.5) stems from insufficient validation when following symbolic links with the ``aiohttp.web.static(follow_symlinks=True)`` option, where an attacker can craft requests to access unauthorized files outside the intended directory structure, potentially compromising sensitive server data.

A publicly available Proof of Concept (PoC) for the CVE-2024-23334 exploit, accompanied by a detailed [YouTube](#) video, was released on February 27th, which was followed by rapid exploitation attempts.

[Cyble Global Sensor Intelligence \(CGSI\)](#) detected scanning activity targeting this vulnerability just a day later, on February 29th, and the activity has been ongoing since, which indicates that threat actors (TAs) were quick to leverage the publicly available information to exploit vulnerable systems.

**Source :** <https://cybersecuritynews.com/shadow-syndicate-aiohttp-vulnerability-data-theft/>



**“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