QUALYSEC
BEYOND CYBERSECURITY

2024

FEB 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com

☎ 865 866 3664

contact@qualysec.com

Fortinet Warns of Critical SSL VPN Flaw Exploited Actively in the Wild

Fortinet has issued a warning regarding a critical out-of-bounds write vulnerability in FortiOS.

Remote attackers can exploit this vulnerability to execute arbitrary code, posing a significant security threat.

A vulnerability known as CVE-2024-21762 (with a CVSSv3 Score of 9.6) can be taken advantage of through a specific type of HTTP request. This vulnerability enables an attacker to execute code or commands using custom-crafted requests.

Fortinet has suggested disabling SSL VPN as a workaround to address the security vulnerability affecting SSL VPN web portals. It is important to note that disabling web mode alone is not a valid workaround. Fortinet has warned that hackers are actively exploiting the vulnerability in question. Significantly, the exploitation is not limited to theoretical attacks but occurs in real-world scenarios.

FortiSIEM recently addressed several OS command injection vulnerabilities, namely CVE-2024-23108 and CVE-2024-23109, prompting an advisory release. According to the latest reports, Chinese state-sponsored hackers recently took advantage of a zero-day vulnerability (CVE-2022-42475) in Fortinet's virtual private network to gain unauthorized access to the Dutch defense networks.

Source : https://cybersecuritynews.com/fortinet-ssl-vpn-flaw-exploited/

US Disrupts Chinese Botnet that Hijacks SOHO Routers

In a decisive action, the U.S. The Department of Justice (DOJ) has disrupted a cyber operation by Chinese state-sponsored hackers.

This operation, codenamed Volt Typhoon, targeted American critical infrastructure using a vast network of compromised routers.

Hundreds of small office/home office (SOHO) routers, primarily Cisco and NetGear models past their "end-of-life" status, were infected with the "KV Botnet" malware. This malware served as a hidden gateway, allowing the attackers to conceal their activities and target critical infrastructure across the nation.

Taking Back Control: A Court-Authorized Cleanup: Through a landmark court order, the DOJ conducted a meticulous operation to dismantle this cyber threat. The compromised routers were remotely accessed and cleansed of the malicious software.

Additionally, measures were taken to sever their connection to the botnet, effectively neutralizing them as tools for further attacks.

A Multi-Pronged Defense: This operation went beyond mere malware removal. The DOJ and its partners, including the FBI, CISA, and private sector entities, are proactively safeguarding critical infrastructure and educating the public.

Source :https://cybersecuritynews.com/us-disrupts-chinese-botnet/

Beware of Fake LastPass Password Manager App That Steals Personal Information

Customers of LastPass have been alerted of a fraudulent app on the Apple App Store that poses as the legitimate LastPass app in an attempt to steal personal data.

Instead of being called "LastPass," the app is called "LassPass," and Parvati Patel is listed as the developer. The app's icon, user interface, and branding are remarkably similar to those of LastPass, which is available in the App Store.

"The app attempts to copy our branding and user interface, though close examination of the posted screenshots reveals misspellings and other indicators the app is fraudulent," reads the LastPass alert.

Specifics of the Fraudulent Application in App Store

The application makes an effort to mimic its interface and logo, but taking a close look at the screenshots that have been shared reveals mistakes and other signs that the application is fake. The fraudulent application has one rating, whereas the legitimate app has 52.3K ratings.

"We are bringing this to our customers' attention to avoid potential confusion and/or loss of personal data," said Mike Kosak, Senior Principal Intelligence Analyst.

Source : https://cybersecuritynews.com/fake-lastpass-password-manager/

Chinese Hackers Remain Undetected in US Infrastructure Systems for Five Years

Volt Typhoon, the PRC state-sponsored threat actor, has been discovered to be compromising U.S. critical infrastructure for future crises in case of a conflict with the United States. The CISA has released a security advisory for warning critical infrastructure organizations about their observations of the Volt Typhoon.

Moreover, the security advisory also confirms that Volt Typhoon has also compromised multiple IT environments belonging to several critical infrastructure organizations in industries such as Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam.

Chinese Hackers Remain Undetected

The Volt Typhoon uses living off-the-land techniques while targeting critical infrastructures. The threat group also uses valid accounts and operational security to maintain persistent access.

The U.S. authoring agencies confidently stated that the threat actor had access to some victim IT environments for at least 5 years. The threat actor seemed to have performed extensive exploitation reconnaissance to understand the targeted organization and its environments.

Source : https://cybersecuritynews.com/chinese-hackers-us-infrastructure/

Ransomware Payments Hitting Record High, Exceed $1 Billion

Chainalysis, a leading blockchain analysis firm, has recently released a report on ransomware payments revealing that they have skyrocketed to a whopping $1 billion in 2023.

This alarming trend sheds light on the increasing menace of cybercrime and highlights the urgent need for enhanced security measures to curb such malicious activities.

In 2023, there was a significant increase in ransomware attacks targeting various industries, including hospitals, schools, and high-profile organizations like British Airways.

These attacks were executed using advanced techniques and tactics, causing severe damage to the affected systems, resulting in data loss, system downtime, and financial losses.

The attackers leveraged sophisticated encryption algorithms, making it difficult for the organizations to recover their data without paying the ransom.

These cybercriminals extorted a staggering $1 billion from their victims, highlighting the growing threat they pose.

The Big Game Hunters:

Now, ransomware gangs like Cl0p target fewer victims but demand millions in ransom, often using stolen data as leverage.

Source : https://cybersecuritynews.com/ransomware-payments-exceed-1-billion/

ANY.RUN Sandbox Now Analyzes Complex Linux Malware For SOC & DFIR Teams

The ANY.RUN sandbox has recently undergone an update to include support for Linux, strengthening its capacity to offer a safe and isolated atmosphere for examining malware and conducting threat analysis. The latest feature introduced will facilitate security analysts to scrutinize and replicate malevolent actions in Linux-oriented systems, providing a more extensive and potent threat perception and response.ANY.RUN is a cloud-based environment for analyzing Windows malware and Linux-based samples. It's useful for malware analysts, SOC, DFIR teams, and SOC personnel with ANY.RUN, users can safely examine threats, simulate different scenarios, and gain insights into malware behavior to improve cybersecurity strategies.

Linux malware analysis is necessary because Linux is a popular target for hackers, and Linux malware is sophisticated.

Linux is widely used in organizational IT infrastructures, resulting in many files that need to be analyzed on these systems.

Researchers at IBM have noticed an increase in Linux malware. In 2020, the number of malware families related to Linux increased by 40%.Compromising Linux-based cloud computing platforms could allow attackers access to massive resources, making the OS an appealing target.

Source : https://cybersecuritynews.com/any-run-sandbox-analyzes-linux-malware/

Spyware Vendors Behind 50% of 0-day Exploits: Google Said

Spyware is a crucial tool for the surveillance and data collection of high-risk individuals. The functionalities of spyware have undergone significant advancements and have become more sophisticated than ever before.

Commercial surveillance vendors (CSVs) offer state-of-the-art spyware technology to governments and private companies, which can exploit security vulnerabilities to surveil individuals.

CSVs pose a significant threat to Google users, as half of all known 0-day exploits against Google products and Android devices can be attributed to them.

CSVs Behind 50% of 0-day Exploits

Google has recently published a comprehensive report that meticulously outlines 40 companies involved in spyware development, sales, and deployment. The report offers detailed insights into the practices of these entities and their contribution to the spyware industry.

Google has discovered that several less popular CSVs were crucial in developing highly advanced spyware.

The use of spyware by governments is becoming outdated as the private sector is now leading in the development of highly advanced tools. Google Threat Analysis Group has identified that many of these sophisticated tools are now being created by the private sector.

Source :https://cybersecuritynews.com/spyware-vendors-0-day/

CYBER SECURITY NEWS

Chinese Hackers Exploited Fortinet Zero-day Flaw to Hack Dutch Defense Networks

Chinese state-sponsored hackers exploited a zero-day vulnerability (CVE-2022-42475) in Fortinet's virtual private network to gain unauthorized access to the Dutch defense networks. The hackers then deployed COATHANGER malware, a sophisticated tool to establish persistence. The Dutch Ministry of Defence reported that their internal computer network was breached by hackers last year. The nature and extent of the breach have not yet been disclosed.

According to the Military Intelligence and Security Service and General Intelligence and Security Service, the hacking incident was caused by Chinese state actors with high certainty. The threat actor conducted network surveillance and retrieved a list of user accounts from the Active Directory server. Fortinet issued a critical advisory in December 2022, warning of a zero-day vulnerability being exploited by an "advanced actor" in attacks on "governmental or government-related targets."The Military Intelligence and Security Service (MIVD) and the General Intelligence and Security Service (AIVD) have conducted an assessment indicating that the malicious activity was carried out by a state-sponsored entity from the People's Republic of China, with a high level of confidence.

Source : https://cybersecuritynews.com/chinese-hackers-fortinet-zero-day/

Linux Shim Bootloader Flaw Expose Most Linux Distros to Code Execution Attacks

Shim is a small application used by open-source projects and other third parties for verifying and running the bootloader (typically GRUB2). The application was developed specifically to circumvent legal issues arising from license compatibility.

Shim has become a critical piece of software for many Linux distributions to support secure boot. However, it has been discovered with a new vulnerability related to out-of-bounds written in HTTP protocol handling that could allow a threat actor to compromise a victim machine completely. This vulnerability has been assigned with CVE-2023-40547, and the severity has been given as 9.8 (Critical).

Shim Bootloader Flaw

Shim is maintained by Red Hat and used in almost all Linux distributions that support secure boot, including Debian, Ubuntu, SUSE, and many others. Along with this vulnerability, five other vulnerabilities were also identified, all of them with medium and high severities.

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

Two New FortiSIEM Max-severity Flaw Let Attackers Execute Remote Code

FortiSIEM has been discovered with multiple OS command injection vulnerabilities, which could allow an unauthenticated remote threat actor to execute unauthorized commands on FortiSIEM via crafted API requests.

The CVEs for these vulnerabilities have been assigned with CVE-2024-23108 and CVE-2024-23109. The severity of these vulnerabilities was given as critical (>=9.8). However, Fortiguard has fixed all the vulnerabilities.

Fortinet has provided a link to its own advisory to furnish additional information. However, when users attempt to access the link, they are directed to an outdated issue that was previously addressed in early October 2023. It is recommended that users seek alternative sources of information until an updated advisory is made available.

CVE-2024-23108 & CVE-2024-23109: Improper Neutralization of Special Elements

These vulnerabilities exist due to an improper neutralization in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2.

Source : https://cybersecuritynews.com/fortisiem-max-severity-flaw/

Google’s Open-source Tool Bazel Flaw Let Attackers Insert Malicious Code

Bazel, an open-source software used for automation of building and testing, has been discovered with a critical supply chain vulnerability that could allow a threat actor to inject malicious code into the Bazel codebase, create a backdoor, and affect the production environment of anyone that uses Bazel.

Researchers stated that millions of projects that use Bazel, such as Kubernetes, Angular, Uber, LinkedIn, Databricks, Dropbox, Nvidia, Google, and many more, could have been affected due to this vulnerability. However, this vulnerability was reported to Google, and the vulnerable workflow has been updated, which fixed it.

Google’s Open-source Tool Bazel Flaw

Bazel has been most widely used in multiple projects and has more than 21,000 stars on GitHub. Additionally, Bazel uses GitHub actions for testing and building new code, labeling issues, and running scheduled tasks.

Three actions interact with the build pipeline with custom actions.

- Docker actions:
- JS actions:

Source : https://cybersecuritynews.com/googles-open-source-bazel-flaw/

CYBER SECURITY NEWS

Hackers Stolen 2M+ User's Data Via XSS & SQL Injection Attacks

A large-scale cyber attack was launched to steal and market confidential user information, focusing mainly on the APAC region's employment agencies and retail firms.
A group of hackers called ResumeLooters initiated a campaign aimed at job seekers. The hackers' identities remain unknown, and their primary objective was to target and exploit vulnerabilities in the job-seeking process.

Group-IB, a cybersecurity company, recently discovered that a group of hackers, ResumeLooters, compromised 65 websites during November and December 2023.

Like GambleForce, ResumeLooters primarily targets the Asia-Pacific – over 70% of known victims are located in the region (India, Taiwan, Thailand, Vietnam, and other countries, as seen below in Figure 2).ResumeLooters SQL injection & XSS as Attack Vectors
The threat actor attempts to steal user databases that may include names, phone numbers, emails, DOBs, information about job seekers' experience, employment history, and other sensitive personal data.

Source : https://cybersecuritynews.com/resumelooters-injection-attacks/

“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

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