QUALYSEC

BEYOND CYBERSECURITY

2024

April 2nd week

CYBER SECURITY NEWS

CONTACT US

🌐 www.qualysec.com

☎ +91 865 866 3664

✉ contact@qualysec.com

CYBER SECURITY NEWS

DuckDuckGo Launches Privacy Pro : 3-In-1 Service With VPN

DuckDuckGo is a search engine that takes users' privacy seriously. It does not track or store personal information.

For those who value their privacy, DuckDuckGo stands out because it does not monitor browsing activities and guarantees a safer and more private internet surfing platform than mainstream players like Google.

Recently, DuckDuckGo launched 'Privacy Pro,' a 3-in-1 service with a VPN.

DuckDuckGo Privacy Pro

DuckDuckGo's Privacy Pro packs an anonymous VPN, Personal Information Removal from data brokers, and Identity Theft Restoration services within it with the following price tags:-

- $9.99 per month
- $99.99 per year

Offering speed, security, and simplicity across five devices simultaneously, this comprehensive privacy solution combines protections that might cost more than $30 when procured from different providers.

Currently, it's only available to U.S. residents, but DuckDuckGo has expansion plans for the future.

Source : https://cybersecuritynews.com/duckduckgo-launches-privacy-pro/

Wiz to Acquire Gem Security for $350M to Address Cloud Security

Wiz, a leading cloud security company, has announced its acquisition of Gem Security for $350 million.

This acquisition marks a significant milestone in Wiz's journey, which began just four years ago when its founders left Microsoft with a vision to reinvent cloud security.

Wiz's story is one of rapid growth and innovation.

Since its inception, the company has been on a mission to revolutionize risk reduction in the cloud.

Wiz's approach to cloud security has resonated with the industry, setting new standards for security and development teams across the Fortune 100 and burgeoning cloud-native companies.

The Acquisition of Gem Security

The acquisition of Gem Security is a testament to Wiz's commitment to expanding its cloud security solutions.

Gem Security's expertise in Cloud Detection and Response (CDR) is poised to complement Wiz's existing offerings, addressing the next wave of security challenges faced by organizations.

Gem Security brings to the table an unmatched understanding of cloud threats.

Source : https://cybersecuritynews.com/wiz-to-acquire-gem/

Critical Bitdefender Vulnerabilities Let Attackers Gain Control Over System

Bitdefender GravityZone Update Server (versions 6.36.1, Endpoint Security for Linux 7.0.5.200089, and Endpoint Security for Windows 7.9.9.380) is vulnerable to server-side request forgery (SSRF) due to an incorrect regular expression.

The weakness allows an attacker to send crafted requests to the server that will be misinterpreted as legitimate. The server, tricked by the irregular expression, will then unknowingly execute those requests.

In the context of SSRF, these requests can be designed to retrieve confidential data from internal systems, manipulate internal configurations, or even pivot to other parts of the network.

In this case, a successful exploit could allow an attacker to reconfigure the update relay, potentially disrupting update delivery or injecting malicious updates into the network.

Bitdefender's GravityZone

Bitdefender's GravityZone Update Server has a critical vulnerability (CVSS score: 8.1) that could allow an attacker remote access (attack vector: network) to compromise the server with low privileges (privileges required: none).

The vulnerability complexity is high (attack complexity: high), meaning it may require specialized skills or knowledge to exploit, where an exploit may already exist (temporal score not provided), and there is no user interaction necessary (user interaction: none) to take advantage of this vulnerability.

Source : https://cybersecuritynews.com/bitdefender-vulnerabilities-attack-control/

Ukrainian Hackers Hijacked 87,000 Sensors to Shut down Sewage System

Ukrainian hackers have successfully infiltrated and disabled a vast network of industrial sensors and monitoring infrastructure in Russia, leading to a significant shutdown of sewage systems, among other utilities.

The group, known as BlackJack, executed the attack on the 9th of April, 2024, causing widespread disruption to Russia's essential services.

The initial breach occurred in June 2023, when the hackers gained access to Russia's Network Operation Center (NOC). The NOC oversees the functioning of various utilities, including gas, water, and fire alarm systems.

The NOC is a critical infrastructure component that controls a network of remote sensors and Internet of Things (IoT) controllers.

The attack has led to the disabling of approximately 87,000 sensors and controls across Russia.

This includes systems within airports, subways, and gas pipelines.

However, the hackers claim to have carefully excluded targets that could affect civilian safety, such as hospitals and airports.

The Malware: Fuxnet

The hackers deployed a potent malware, dubbed 'Fuxnet'—a reference to the infamous Stuxnet worm, but with enhancements.

Fuxnet was designed to cause physical damage to the sensory equipment by exhausting NAND/SSD memory and corrupting firmware with wrong CRC values.

· **Source : https://cybersecuritynews.com/ukrainian-hackers-hijacked/**

Zscaler Acquires Airgap Networks to Enhance Zero Trust SASE

Zscaler has announced the acquisition of Airgap Networks, a company renowned for its agentless segmentation technology.

This acquisition is set to redefine the way enterprises protect their internal traffic, particularly in IT and Operational Technology (OT) environments.

Cybersecurity rapidly evolves, with adversaries employing sophisticated techniques to bypass traditional security measures.

Once inside a network, these attackers move laterally to access sensitive data or critical resources. To combat this, zero-trust security models have become essential, focusing on the principle of "never trust, always verify."

Historically, network segmentation has been the go-to strategy for controlling lateral movement within networks.

However, traditional methods like Network Access Control (NAC) and East-West firewalls have proven complex and cumbersome, often leading to misconfigurations and incomplete implementations.

Zscaler recently announced on Twitter its plan to acquire Airgap, which will enhance the company's Zero Trust Secure Access Service Edge (SASE).

Source : https://cybersecuritynews.com/zscaler-acquires-airgap/

Critical Node.js Flaw Lets Attackers Execute Malicious Code on Windows Machines

Node.js project disclosed a high-severity vulnerability affecting multiple active release lines of its software on Windows platforms.

This flaw, identified as CVE-2024-27980, allows attackers to execute arbitrary commands on affected systems, posing a serious risk to applications and services built on Node.js.

Node.js Flaw Lets Attackers Execute Malicious Code

The core of the vulnerability lies within the child_process.spawn and child_process.spawnSync functions of Node.js when used on Windows operating systems. These functions are commonly utilized to spawn child processes from Node.js applications.

The flaw was discovered in the handling of batch files and command-line arguments passed to these functions.

Specifically, it was found that a maliciously crafted command-line argument could lead to command injection and arbitrary code execution, even if the shell option is not enabled in the function call.

This vulnerability is particularly alarming because it bypasses the safety mechanism provided by disabling the shell option, which is often recommended as a security best practice.

The impact is widespread, affecting all users of the 18.x, 20.x, and 21.x release lines of Node.js on Windows.

Source : https://cybersecuritynews.com/node-js-flaw-malicious-code/

Multiple Palo Alto Networks Firewall Flaws Let Attackers Cause Disruption

Palo Alto Networks has recently disclosed four high-severity vulnerabilities in its firewall products.

If exploited, these flaws could allow attackers to disrupt services by causing a denial of service (DoS) or manipulating user access controls. The vulnerabilities are tracked as CVE-2024-3382, CVE-2024-3383, and CVE-2024-3384.

CVE-2024-3382: Denial of Service via Crafted Packets

The first vulnerability, CVE-2024-3382, affects the PAN-OS operating system and can lead to a denial of service (DoS) condition when the firewall processes a burst of specially crafted packets. This issue specifically impacts PA-5400 Series devices with the SSL Forward Proxy feature enabled. Palo Alto Networks has addressed this flaw in PAN-OS versions 10.2.7-h3, 11.0.4, 11.1.2, and later.

CVE-2024-3383: Improper Group Membership Change

CVE-2024-3383 is a vulnerability in the Cloud Identity Engine (CIE) component of PAN-OS, which could allow unauthorized changes to User-ID groups. This flaw could lead to inappropriate access control decisions, affecting the security of network resources. The company has fixed this issue in PAN-OS versions 10.1.11, 10.2.5, 11.0.3, and all subsequent releases.

Source : https://cybersecuritynews.com/palo-alto-networks-firewall-flaws/

AT&T Breach Update: 51 Million Customers' Data Exposed

AT&T has confirmed that a data breach has impacted the personal information of 51 million current and former customers.

A significant data breach has been uncovered in recent times, following a series of investigations and reports. The scale of the cybersecurity incident was gradually revealed, making it one of the most substantial breaches in recent years.

The breach first came to light in March 2024 when a dataset containing sensitive customer information was discovered on the dark web.

Initial reports suggested that the data included personal details such as Social Security numbers, email addresses, phone numbers, and birth dates, affecting current and former account holders.

AT&T conducted an investigation and determined that the data that was breached seems to have originated from June 2019 or an earlier date. The company made efforts to identify the source of the breach, but it's still unclear how the attackers were able to access the data.

AT&T has told Marine AG that there is no evidence of unauthorized access to its systems, which results in the exfiltration of the dataset.

Source : https://cybersecuritynews.com/att-breach-update/

Financial Sectors Lost $20 Billion Over the Past 20 Years

In a startling revelation, cyberattacks have surged to more than double their pre-pandemic levels, casting a long shadow over global financial stability.

The International Monetary Fund (IMF) highlighted this alarming trend in its April 2024 Global Financial Stability Report, underscoring the escalating risk of catastrophic financial losses due to cyber incidents.

Historically, direct financial losses from cyberattacks on companies have been relatively contained. However, certain cases have demonstrated the potential for devastating financial repercussions.

A notable example is the US credit reporting giant Equifax, which incurred over $1 billion in penalties following a significant data breach in 2017, impacting approximately 150 million consumers.

The IMF report draws attention to the growing magnitude of potential losses, which have seen a staggering increase. The cost of extreme cyber incidents has quadrupled since 2017, reaching an unprecedented $2.5 billion. These figures do not account for the indirect costs associated with such attacks, which include reputational damage and the expenses related to bolstering security measures.

Source : https://cybersecuritynews.com/financial-sectors-lost-20-billion-over-the-past-20-years/

Multiple Adobe Security Vulnerabilities Let Attackers Execute Arbitrary Code Remotely

A product security incident response team (PSIRT) manages a vulnerability disclosure program by acting as a single point of contact for external reporters, including customers, partners, penetration testers, and security researchers.

They provide a standardized process for reporting security vulnerabilities found in the organization's products and services. They prioritize private disclosure conducted in a way that minimizes risk to user data, the organization's infrastructure, and its reputation.

Vulnerability Details

Security updates are available for Adobe Experience Manager (AEM) to address critical vulnerabilities that attackers could exploit to execute arbitrary code or bypass security features, as all versions of AEM Cloud Service (CS) and AEM 6.5.19.0 and earlier are affected.

To mitigate the risks, administrators are recommended to update AEM to either AEM Cloud Service Release 2024.03 or AEM 6.5 Service Pack 20.0, both of which address the identified vulnerabilities.

The security updates have been released to address critical vulnerabilities in Adobe Premiere Pro for Windows and macOS that could be exploited to execute arbitrary code on an affected system.

Source : https://cybersecuritynews.com/adobe-security-flaws-remote-execution/

Cypago Announces New Automation Support for AI Security and Governance

Cyber GRC software company Cypago has announced a new automation solution for artificial intelligence (AI) governance, risk management and compliance. This includes implementation of NIST AI RMF and ISO/IEC 42001, the newest AI security and governance frameworks. With more and more companies integrating new AI tools into their business processes, daily operations, and customer-facing products and services, safe and compliant use of AI has become a pivotal challenge.

Enterprises are adopting AI-powered tools and solutions at a staggering pace, thanks to the increasing power and democratization of AI platforms, and the extensive benefits that artificial intelligence can bring to business operations. However, AI also brings many dangers, including the potential for leaking private data, lack of transparency, and increasingly complex cyber threats. Organizations also need to prepare themselves for more legislation regulating the use and application of AI in business settings.

The best way to protect against these dangers and stay ahead of AI regulations is through adherence to best practices for cyber GRC governance, which are in a constant state of flux. By providing comprehensive risk management, automated 24/7 monitoring, and cybersecurity governance tailored to AI solutions, Cypago enables companies to seamlessly secure their AI initiatives.

Source : https://cybersecuritynews.com/cypago-announces-new-automation-support/

CYBER SECURITY NEWS

Mysterious Index Bug Haunts a Tech Company's Search Engine Project

A mysterious bug has plagued a major tech company's search engine project since February, randomly failing the index construction process. The issue is related to the code that merges partial indices during index building.

"The search engine constructs the reverse index through successive merging of smaller indices to reduce memory requirements," explained lead engineer Jane Doe. "Suddenly, the code that merges these indices started failing randomly."

The Bug's Impact on Index Construction

The search engine operates by creating a reverse index through the successive merging of smaller indices, a process that is essential for reducing memory requirements.

The reverse index comprises two files: one containing offset pointers and another with sorted numbers. This process is initiated after each partition completes its crawling and processing, typically taking around four hours to run.

However, developers encountered a sudden and random failure in the code responsible for merging the indices.

The failure occurred when copying sorted numbers from an older index to a newer one, in cases where a keyword was present in only one of the indexes, thus not requiring an actual merge.

Source : https://cybersecuritynews.com/mysterious-index-bug-in-search-engine-project/

“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