REDRABBIT SECURITY

About us

The internet is a dangerous place, and it's only becoming more dangerous. Red Rabbit Security provides managed security services to protect your data and your business from cyber threats. Whether you're looking for web security, email security, or network security, we have you covered.

Red Rabbit Security has one of the most experienced teams in the industry, with experts who are constantly staying up-to-date with the latest trends and techniques in cyber security. Our team is dedicated to proactively identifying and mitigating potential threats, ensuring that your business remains secure in an ever-evolving digital landscape. Trust Red Rabbit Security to safeguard your valuable assets and provide you with peace of mind.

Get a Free Cyber Security Assessment

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. III

REDRABBIT SECURITY

Cyber Headlines

UK Ministry of Defence Slapped with $440K Fine Over Afghan Evacuation Data Breach

In a shocking revelation, the UK Ministry of Defence faces a hefty £350,000 (approximately $440,000) fine for a data breach during the Afghan evacuation crisis in 2021. The Information Commissioner's Office (ICO) decried the failure to protect sensitive information of Afghans seeking relocation, emphasizing that the mistake "could have resulted in a threat to life." The breach occurred when an email containing the personal details of 245 individuals eligible for evacuation was mistakenly sent to a list of Afghan nationals.

The exposed information, visible to all recipients, posed a serious risk to lives, potentially falling into the hands of the Taliban. The ICO criticized the Ministry's security lapses and highlighted the vulnerability of using 'blind carbon copy,' reducing the fine from £1,000,000 to £350,000 due to its impact on the public sector. The incident sheds light on the critical need for robust data protection measures during sensitive operations.

Read more about the article https://therecord.media/uk-defence-fined-for-afghan-breach?&web_view=true to delve into the details of this alarming breach and its implications for national security.

IN THIS ISSUE

REDRABBIT SECURITY

Cyber Headlines

Critical Bluetooth Flaw Puts Millions of Devices at Risk of Takeover

In a shocking revelation, a critical Bluetooth security flaw, identified as CVE-2023-45866, has emerged as a potential threat to the security of Android, Linux, macOS, and iOS devices. Unearthed by security researcher Marc Newlin, the flaw centers around an authentication bypass that allows threat actors to seize control by injecting keystrokes, leading to code execution on the victim's device. The exploit takes advantage of an "unauthenticated pairing mechanism" within the Bluetooth specification, tricking the target device into believing it's connected to a Bluetooth keyboard. Disturbingly, this attack, which doesn't require specialized hardware, can be executed from a Linux computer using a standard Bluetooth adapter.

This vulnerability, affecting a wide array of devices dating back to Android version 4.2.2 from November 2012, poses a serious risk to user privacy and data security. Notably, even Apple's LockDown Mode, designed to thwart sophisticated digital threats, is not immune. Google has issued a warning, stating that the flaw could result in remote escalation of privilege without the need for additional execution privileges, emphasizing the urgent need for users to update their devices and remain vigilant against potential exploits.
https://thehackernews.com/2023/12/new-bluetooth-flaw-let-hackers-take.html

IN THIS ISSUE

REDRABBIT SECURITY

Cyber Headlines

UK Government Faces Imminent Threat of "Catastrophic Ransomware Attack," Urgent Report Warns

A parliamentary committee report has issued a stark warning about the imminent risk of a "catastrophic ransomware attack" that could bring the UK to a standstill. The report underscores the potential devastating impact on citizens, the economy, and national security, urging immediate action to address the inadequacies in the government's cybersecurity measures. With outdated infrastructure and vulnerable supply chains identified as key concerns, the report calls for increased funding for the National Cyber Security Center to fortify defenses against cyber threats.

As cyberattacks on critical infrastructure escalate globally, the UK finds itself as the third most targeted country, facing threats from state-aligned groups sympathetic to Russia's actions. Governments worldwide are urged to prioritize cybersecurity to counter the growing sophistication of attackers. The report concludes with a plea for a proactive stance to prevent "catastrophic costs."

Read more about the news here :
https://www.csoonline.com/article/1258591/uk-government-vulnerable-to-catastrophic-ransomware-attack-report.html

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. III

REDRABBIT SECURITY

Did You Know

➢ **Did you know?** that in 2022, a staggering 10 million secrets were found leaked on GitHub, representing a 67% increase from the previous year? These leaked secrets, including API keys and developer credentials, pose a significant security risk, emphasizing the need for continuous vigilance and proactive measures to safeguard sensitive data, especially in sectors like healthcare facing persistent cyber threats.

➢ **Did you know?** That Electronic Health Records (EHRs) can command up to $1,000 each on the dark web, making them significantly more valuable than credit card numbers or social security numbers, highlighting the healthcare industry's attractiveness to cybercriminals?

➢ **Did you know?** That adversaries are increasingly leveraging OAuth applications to automate virtual machine deployment for cryptocurrency mining and phishing attacks?

➢ **Did you know?** That according to a study by the Security Industry Association (SIA), 93% of security industry business leaders expect generative artificial intelligence (AI), such as ChatGPT, to impact their business strategies within the next 5 years, highlighting the widespread anticipation of AI's influence in the security segment?

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. III

REDRABBIT SECURITY

Threat Intelligence

Critical Vulnerabilities Plague pfSense Instances, Leaving Over 1,400 Systems at Risk

Alarming threat intelligence reveals that approximately 1,450 instances of pfSense, a widely used open-source firewall and router software, are exposed online and susceptible to command injection and cross-site scripting (XSS) vulnerabilities. Discovered by SonarSource researchers in mid-November, these flaws, tracked as CVE-2023-42325, CVE-2023-42327, and CVE-2023-42326, affect pfSense versions 2.7.0 and older, as well as pfSense Plus 23.05.01 and older.

The severity of the command injection flaw, with a CVSS score of 8.8, allows threat actors to execute remote code with root privileges. While Netgate, the vendor of pfSense, promptly released security updates in November, nearly 92.4% of the exposed instances remain vulnerable, posing a significant threat to large enterprises that rely on pfSense. This exposes a potential attack surface, enabling threat actors to leverage high-level privileges within compromised networks, leading to data breaches and unauthorized access to sensitive resources.

Read more about the critical vulnerabilities affecting pfSense instances and the potential risks associated with this widespread threat https://www.bleepingcomputer.com/news/security/over-1-450-pfsense-servers-exposed-to-rce-attacks-via-bug-chain/?&web_view=true.

IN THIS ISSUE

REDRABBIT SECURITY

Threat Intelligence

BazaCall Phishing Tactics Evolve: Threat Actors Exploit Google Forms for Deceptive Authenticity

In a concerning evolution of the BazaCall phishing attacks, threat actors are now utilizing Google Forms to enhance the scheme's credibility, as reported by cybersecurity firm Abnormal Security. BazaCall, active since 2020, involves phishing emails impersonating subscription notices, urging recipients to contact a support desk urgently. The latest variant involves creating a Google Form that appears as a payment confirmation for Norton Antivirus software, exploiting the trust associated with the Google domain. The dynamic nature of Google Forms' URLs adds another layer of evasion against traditional security measures relying on static analysis and signature-based detection.

Meanwhile, Proofpoint has uncovered a new phishing campaign targeting recruiters, attributed to the financially motivated threat actor TA4557. This sophisticated attack employs direct emails leading to a JavaScript backdoor known as More_eggs. Once recipients reply, they receive URLs to a fake resume website or attachments containing instructions, ultimately delivering the More_eggs malware.

https://thehackernews.com/2023/12/bazacall-phishing-scammers-now.html

IN THIS ISSUE

REDRABBIT SECURITY

Released Patches and Updates

Microsoft Concludes 2023 with Final Patch Tuesday, Addressing 33 Flaws

Microsoft has rolled out its last set of Patch Tuesday updates for 2023, tackling a total of 33 vulnerabilities in its software. This release stands out as one of the lighter ones in recent years, addressing four critical and 29 important flaws. While none of the vulnerabilities are currently known to be under active attack, notable issues include a Windows MSHTML Platform Remote Code Execution Vulnerability (CVE-2023-35628) and an Internet Connection Sharing (ICS) Remote Code Execution Vulnerability (CVE-2023-35630). Another significant flaw, CVE-2023-36019, affecting Microsoft Power Platform Connector, allows attackers to execute malicious scripts in the victim's browser by manipulating a specially crafted URL. As organizations apply these patches.

The update also addresses three flaws in the Dynamic Host Configuration Protocol (DHCP) server service, including denial-of-service and information disclosure vulnerabilities. With this final Patch Tuesday release, organizations are urged to promptly apply the updates to mitigate potential risks associated with these vulnerabilities. Stay updated on the latest patches and address vulnerabilities promptly to bolster your system's security.
https://thehackernews.com/2023/12/microsofts-final-2023-patch-tuesday-33.html

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. III

REDRABBIT SECURITY

Released Patches and Updates

Kali Linux 2023.4 Released: New Tools and GNOME 45 Desktop

Kali Linux, the go-to Linux distribution for ethical hackers and cybersecurity professionals, has launched its final version for 2023, featuring fifteen new tools and the GNOME 45 desktop environment. While core operating system additions are limited, the update includes critical tools such as cabby, Havoc, and Portspoof. Kali Linux 2023.4 also introduces GNOME 45, offering enhanced features like full-height sidebars, improved search speed in the Nautilus file manager, and updated themes.

The Kali Team emphasizes the importance of prompt updates for users, presenting various deployment options, including Amazon AWS, Microsoft Azure, Hyper-V, and Raspberry Pi 5. Existing users can easily upgrade using simple commands provided by Kali Linux.

IN THIS ISSUE

REDRABBIT SECURITY

Webinars, Conference, and Events

Vision 2024: Looking Ahead at Cyber Threats

Cybersecurity professionals are coming together for the second annual Vision conference to learn about the newest industry trends, discuss predictions for what's coming in cybercrime, and understand how to best keep their organizations protected in the new year. Register for Vision 2024 to interact with and learn from leading cyber and AI experts on: • AI and Cybersecurity Today: Discover the good, the bad, and how to use AI to solve your business problems. • New and Persistent Threats: Identify coming threats and how hackers are improving their efficacy to trick your end-users. • Forward-Thinking Strategies: Learn how you can apply innovative security methods in real-world use cases to strengthen your security posture.

Key Details:

January 11, 2024
Event Duration: 1 Day
Online
Cost: $0

https://futureconevents.com/events/houston-tx-2023/

IN THIS ISSUE

CYBER NEWS

12/2023 Vol. III

REDRABBIT SECURITY

Featured Article of the Week

European Union Lawmakers Reach Landmark Agreement on AI Regulation with the AI Act

On December 8, 2023, European Union lawmakers finalized negotiations on the groundbreaking AI Act, marking a historic effort to regulate artificial intelligence comprehensively. The legislation, once adopted, will set a precedent globally, influencing how tech giants like Google and Microsoft, as well as AI startups, operate within the EU. Designed to protect consumer rights and spur innovation, the AI Act classifies AI systems into tiers, ranging from unacceptable risk to limited and minimal risk, with clear standards for each. Notably, the bill includes cybersecurity implications, emphasizing the need for robust security measures, particularly for high-risk systems. The document addresses various aspects, including bans on social scoring systems, real-time biometric identification, and the use of AI in manipulating election results.

Read more about the attack here:
https://www.csoonline.com/article/1258597/how-the-eu-ai-act-regulates-artificial-intelligence-and-what-it-means-for-cybersecurity.html

IN THIS ISSUE