CYBER NEWS

11/2023 Vol. I

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

www.redrabbitsec.com

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT
SECURITY

Cyber Headlines

Singapore's Public Healthcare System Hit by Devastating DDoS Attacks, Just Five Years After Major Data Breach

The recent cyberattacks on Singapore's healthcare institutions underscore the growing threat to critical infrastructure by cybercriminals. Disruptive distributed denial-of-service (DDoS) attacks not only caused operational havoc but also unveiled vulnerabilities in patient data access and service delivery. amplifying patient anxiety and eroding trust in the system. Occurring after a significant data breach five years prior, these incidents emphasize the urgency of bolstering cybersecurity measures.

A holistic approach is essential: training healthcare staff, implementing strong security controls, regular system audits, and a robust incident response plan. Cultivating a culture of cybersecurity awareness and educating the public crucial in fortifying defenses against cyber threats. Collaboration among the healthcare sector, government, and public participation is vital to fortify the healthcare system and ensure the uninterrupted delivery of critical services.

For further details and in-depth information on these events, you can find the article in [https://therecord.media/singapore-public-health-services-ddos-attack?&web_view=true] cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT
SECURITY

Cyber Headlines

Healthcare Ransomware Epidemic: US Sees Alarming 60% Surge in Breaches Impacting 88 Million Patients

The Department of Health and Human Services (HHS) unveiled a distressing 60% surge in 2023's breaches, affecting a staggering 88 million individuals, with hacking contributing to 77% of these security compromises. Ransomware's insidious rise poses a significant threat to patient data and service delivery. The HHS report underscores a 239% increase in major breaches over four years, necessitating urgent, robust cybersecurity measures in healthcare.

A recent Sophos report illuminates the complexity: 60% of surveyed healthcare organizations experienced ransomware breaches, and distressingly, only a quarter of these attacks were intercepted before data encryption. This escalation not only disrupts essential medical services, jeopardizing patient care and surgeries, but also imperils sensitive patient information. Hospitals remain prime targets due to their reliance on technology, exacerbating their vulnerability. As these attacks intensify, the critical need for fortified cybersecurity becomes increasingly apparent to safeguard patient safety and data integrity. For further details and in-depth information on these events, you can find the article in [https://www.infosecurity-magazine.com/news/healthcare-data-breaches-88-million/?&web_view=true]

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT SECURITY

Did You Know

➢ **Did you know?** According to the Department of Health and Human Services, there has been a staggering 239% increase in "large breaches" reported to its Office for Civil Rights (OCR) over the past four years. Additionally, ransomware attacks have surged by 278% during the same period, highlighting a grave concern for the security of sensitive health data.

➢ **Did you know?** A recent Sophos report uncovered that 60% of surveyed healthcare organizations suffered a ransomware breach in the past year, a slight decrease from 66% in 2022. However, in 75% of these incidents, data was successfully encrypted, indicating the severity and impact of these attacks on sensitive patient information and medical services.

➢ **Did you know?** In Q3 of 2023, global ransomware attacks increased by a significant 11% compared to Q2, marking a striking 95% year-over-year surge, as reported by Corvus Insurance. This uptick underscores the persistent and growing threat posed by ransomware across the globe.

➢ **Did you know?** Despite 96% of organizational leaders claiming at least moderate support and investment in cybersecurity mandates, a concerning trend emerges where 49% of CXOs have sought to bypass one or more security measures within the past year. This discordance between support for cybersecurity and executive actions highlights potential vulnerabilities within organizations.

IN THIS ISSUE

1. Cyber Headlines - Latest cyber news from around the globe.

2. Did You Know - Short and informative cyber security facts and stats.

3. Threat Intelligence - Latest in cyber threat intelligence from across all industries.

4. Newly Released Patches and Updates - Vendor agnostic patches and updates information.

5. Upcoming Webinars, Conferences, and Events - The latest information from around the globe for learning and networking opportunities.

6. Featured Article of the Week - Articles from around the world related to cyber security.

www.redrabbitsec.com

CYBER NEWS

11/2023 Vol. I

REDRABBIT SECURITY

Threat Intelligence

Rapid7 Insight: ActiveMQ Flaw Exploited to Deploy Hello Kitty Ransomware

Cybercriminals have begun exploiting a critical remote code execution vulnerability in Apache ActiveMQ to deploy ransomware on enterprise networks. The vulnerability, tracked as CVE-2023-46604, was patched last week, but attackers have already begun leveraging it to deploy the Hello Kitty ransomware program. Security firm Rapid7 has identified suspected exploitation of CVE-2023-46604 in two different customer environments. In both instances, the attackers attempted to deploy ransomware binaries on target systems in an effort to ransom the victim organizations. Based on the ransom note left behind and other details of the attack, Rapid7 believes the attackers deployed the Hello Kitty ransomware program, whose source code was leaked on underground forums earlier this month.

Apache ActiveMQ is a popular middleware used in developing enterprise software solutions. As such, the exploitation of CVE-2023-46604 poses a significant risk to organizations that utilize this software. The vulnerability stems from insecure deserialization, a common technique used in Java applications. If the original input is not properly sanitized, it can lead to security issues. Organizations are urged to upgrade their Apache ActiveMQ installations to the latest version immediately.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT SECURITY

Released Patches and Updates

Cisco has released several patches to address critical vulnerabilities in its Firepower network security devices, Identity Services Engine (ISE) network access control platform, and Adaptive Security Appliance (ASA). The US Cybersecurity and Infrastructure Security Agency (CISA) has urged administrators to deploy the available patches immediately, warning that these vulnerabilities could allow attackers to take control of affected systems.

The most severe flaw, rated as critical, resides in the Management Center Software of Cisco Firepower and allows an authenticated attacker to send unauthorized configuration commands to Firepower Threat Defense (FTD) devices. By exploiting this vulnerability, an attacker could gain significant control over affected systems. Cisco also patched two other command injection vulnerabilities in the Cisco Firepower Management Center. These flaws allow attackers to execute commands on the underlying operating system but require valid credentials to exploit. A fourth code injection flaw, patched in both the Management Center and Threat Defense software, allows an authenticated attacker to execute commands on the device as root. However, the attacker needs administrator privileges to target the vulnerable system.

Given the severity of these vulnerabilities, CISA has urged administrators to deploy the available patches as soon as possible.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT SECURITY

Webinars, Conference, and Events

Cybersecurity and ransomware live!

Gear up for Cybersecurity & Ransomware Live!, the ultimate cybersecurity conference designed to arm you with the knowledge and skills you need to navigate the ever-changing digital landscape. Join us as we bring together industry experts and seasoned practitioners to tackle the most pressing cybersecurity challenges head-on. This conference equips attendees with the knowledge necessary to succeed in the following areas: ransomware, backup and recovery strategies, cloud-native security, how to defend against contemporary threats, how to notify executive teams of impending security threats, and how to design and deploy applications in hardened environments, and much more.

Key Details:
November
12-17, 2023 | ORLANDO
Royal Pacific
Resort at Universal
Event Page

cont.

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

REDRABBIT SECURITY

Webinars, Conference, and Events

Black Hat Middle East and Africa

Prepare for a transformative experience at Black Hat Middle East and Africa, a paramount cyber security conference and exhibition set to unfold in Riyadh, KSA. This esteemed event unites over 40,000 infosec professionals, hosts 300+ exhibitors, and features 300+ globally recognized speakers from across 120 countries. Join the collaborative effort to leverage cutting-edge technologies and innovative processes to proactively shape a secure future. Engage in knowledge-sharing, exchange proven strategies and glean insights from industry-leading experts within your field, propelling you towards the forefront of emerging developments and current best practices.

Key Details
November 14,
2023 | Riyadh Saudi Arabia
Event
Duration: 3 Days
Event Page

IN THIS ISSUE

CYBER NEWS

11/2023 Vol. I

RED RABBIT SECURITY

Featured Article of the Week

Data Leak Alert: Ransomware Gang Leaks Data Allegedly Stolen From Canadian Hospitals

Five Canadian hospitals have recently disclosed distressing news confirming the leakage of patient and employee data. This sensitive information, which was initially compromised during a ransomware attack, has now been made public. The incident raises significant concerns about data security and highlights the urgency of robust cybersecurity measures to safeguard critical healthcare information.

Discover the full, alarming details and implications of this breach by visiting SecurityWeek.

IN THIS ISSUE