# New Fortinet RCE Flaw in FortiOS SSL VPN Likely Exploited in Attacks

Link: https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/?&web\_view=true

Description: The vulnerability affects various versions of FortiOS, and the recommended solution includes upgrading to specific versions or migrating to a fixed release to address the flaw.

# Ransomware Leak Site Reports Rose by 49% in 2023, but There Is Good News

Link: https://www.zdnet.com/article/ransomware-leak-site-reports-rose-by-49-in-2023-but-there-is-good-news/?&web\_view=true

Description: While ransomware groups targeted a wide range of industries for profit, the demise of several groups in 2023 was attributed to increased pressure from law enforcement and cybersecurity organizations.

# New Zardoor Backdoor Used in Long-Term Cyber Espionage Operation Targeting an Islamic Organization

Link: https://blog.talosintelligence.com/new-zardoor-backdoor/?&web\_view=true

Description: The threat actor maintained long-term access to the victim's network, evading detection by using living-off-the-land binaries, side-loading backdoors, and leveraging open-source reverse proxy tools like Fast Reverse Proxy (FRP) and Venom.

# Google Settles Google+ API Data Leak Lawsuit for $350M

Link: https://www.bankinfosecurity.com/google-settles-google-api-data-leak-lawsuit-for-350m-a-24296?&web\_view=true

Description: The shareholders, led by the state of Rhode Island's retirement system, accused Google of concealing the extent of the data breach and failing to notify users about the API flaw.

# Hyundai Motor Europe Hit by Black Basta Ransomware Attack

Link: https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/?&web\_view=true

Description: Hyundai Motor Europe suffered a Black Basta ransomware attack, resulting in the theft of three terabytes of corporate data, impacting various departments including legal, sales, human resources, accounting, IT, and management.

# Chinese Threat Actors Found Spying on Dutch Defense Ministry Network

Link: https://cyware.com/news/chinese-threat-actors-found-spying-on-dutch-defense-ministry-network-fc1b1020

Description: Chinese state actors used a zero-day exploit in a Fortinet VPN to breach Dutch military systems—in early 2023—to deploy the Coathanger backdoor, revealed intelligence agencies. The malware conceals its activities by intercepting system functions that might expose it. Organizations are urged to enha ... Read More

# Meta Is Being Urged to Crack Down on UK Payment Scams

Link: https://www.bankinfosecurity.com/meta-being-urged-to-crack-down-on-uk-payment-scams-a-24306?&web\_view=true

Description: Banking fraud prevention heads from TSB Bank, Santander, and Revolut testified before a U.K. Parliament committee, highlighting the prevalence of scams on Meta-owned online marketplaces like Facebook Marketplace.

# California Union Confirms Ransomware Attack Following Claims by LockBit

Link: https://therecord.media/california-union-lockbit-attack-ransomware?&web\_view=true

Description: The Service Employees International Union (SEIU) Local 1000 in California is dealing with network disruptions following a cyber incident, which was claimed by the LockBit ransomware gang last month.

# Google Will Block Android Users From Installing ‘Unsafe’ Apps in Fraud Protection Test

Link: https://www.zdnet.com/article/google-will-block-android-users-from-installing-unsafe-apps-in-fraud-protection-test/?&web\_view=true

Description: Google is collaborating with the Singapore government to roll out a new security feature in Google Play Protect to block the installation of potentially risky side-loaded apps, aiming to protect Android users from malware-enabled scams.

# Feds Warn Health Sector About Akira Ransomware Again, Amid New Attacks

Link: https://www.healthcareinfosecurity.com/feds-warn-health-sector-about-akira-again-amid-new-attacks-a-24320?&web\_view=true

Description: The Akira ransomware group poses a significant threat to the U.S. healthcare sector and has targeted organizations in multiple industries, using tactics such as spear-phishing and exploiting vulnerabilities in VPN software.

# Report: Critical Manufacturing Vulnerabilities Surge 230% in Six Months

Link: https://www.infosecurity-magazine.com/news/critical-manufacturing-surge/?&web\_view=true

Description: A new report by Nozomi Networks highlighted an increasing threat to operational technology (OT) and Internet of Things (IoT) environments, with 885 new vulnerabilities disclosed in the second half of 2023.

# Raspberry Robin Actors are Buying Exploits for Faster Attacks

Link: https://www.theregister.com/2024/02/08/raspberry\_robin\_bought\_exploits/?&web\_view=true

Description: The group's access to exploits for vulnerabilities, such as CVE-2023-36802 and CVE-2023-29360, suggests ties to sophisticated developers and the purchase of external 64-bit executables rather than in-house development.

# Security Compass Announces Acquisition of Kontra from ThriveDX

Link: https://finance.yahoo.com/news/security-compass-announces-acquisition-kontra-140000943.html?&web\_view=true

Description: The acquisition reflects Security Compass's commitment to providing top-tier cybersecurity training solutions and complements its existing offerings, including Application Security Training, SD Elements, and Just-In-Time Training.

# Android XLoader Malware can Now Auto-Execute After Installation

Link: https://www.bleepingcomputer.com/news/security/android-xloader-malware-can-now-auto-execute-after-installation/?&web\_view=true

Description: The XLoader Android malware, operated by the threat actor known as Roaming Mantis, has been found to automatically execute on infected devices without requiring user interaction.

# Update: Anydesk Says Software ‘Safe to Use’ After Cyberattack

Link: https://therecord.media/anydesk-software-safe-to-use-cyberattack?&web\_view=true

Description: The cyberattack on AnyDesk's servers in Spain and Portugal did not result in the compromise of user credentials, and the company has taken steps to mitigate the incident.

# Emirates NBD Reportedly Involved in a Data Breach

Link: https://securereading.com/emirates-nbd-reportedly-involved-in-a-data-breach/?&web\_view=true

Description: The criminal organization "Wail Crinal 213" claims to have accessed the bank's server and is allegedly selling sensitive customer data, including emails, usernames, account details, and more.

# Ivanti Publishes Urgent Warning About New Vulnerability

Link: https://therecord.media/ivanti-urgent-warning-new-vulnerability?&web\_view=true

Description: The software company Ivanti has discovered a new vulnerability, CVE-2024-22024, in its products that allows unauthorized access to restricted resources. Although there is no evidence of exploitation, users are urged to promptly patch their systems.

# ResumeLooters Steal Millions of Unique Emails from Multiple Sites

Link: https://cyware.com/news/resumelooters-steal-millions-of-unique-emails-from-multiple-sites-b8f0f81b

Description: ResumeLooters conducted a major cyber operation, compromising over 65 job search and retail websites across the Asia Pacific region and pilfering more than 2 million user records. The discovery of a new campaign serves as a reminder to secure databases and websites—which can be exploited by publicl ... Read More