Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

48th Release March 2023

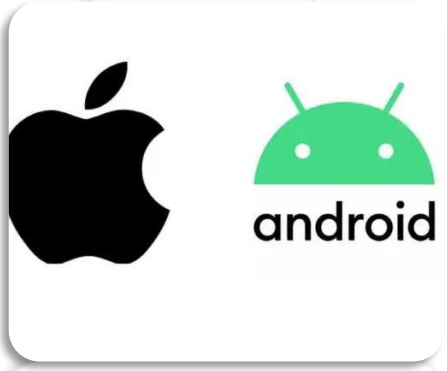
Microsoft Warns of Stealthy Outlook Vulnerability Exploited by Russian Hackers

Microsoft shared guidance to help customers discover indicators of compromise (IoCs) associated with a recently patched Outlook vulnerability.

Tracked as CVE-2023-23397 (CVSS score: 9.8), the critical flaw relates to a case of privilege escalation that could be exploited to steal NT Lan Manager (NTLM) hashes and stage a relay attack without requiring any user interaction.

Microsoft's incident response team said it found evidence of potential exploitation of the shortcoming as early as April 2022.

Source:https://thehackernews.com/2023/03/microsoft-warns-of-stealthy-outlook.html



Spyware Vendors Caught Exploiting Zero-Day Vulnerabilities on Android and iOS Devices

A number of zero-day vulnerabilities that were addressed last year were exploited by commercial spyware vendors to target Android and iOS devices, Google's Threat Analysis Group (TAG) has revealed.

The two distinct campaigns were both limited and highly targeted, taking advantage of the patch gap between the release of a fix and when it was actually deployed on the targeted devices. The scale of the two campaigns and the nature of the targets are currently unknown.

Source:https://thehackernews.com/2023/03/spyware-vendors-caught-exploiting-zero.html

OpenAI Reveals Redis Bug Behind ChatGPT User Data Exposure Incident

OpenAI disclosed that a bug in the Redis open source library was responsible for the exposure of other users' personal information and chat titles in the upstart's ChatGPT service earlier this week.

The glitch, which came to light on March 20, 2023, enabled certain users to view brief descriptions of other users' conversations from the chat history sidebar, prompting the company to temporarily shut down the chatbot.

Source:https://thehackernews.com/2023/03/openai-reveals-redis-bug-behind-chatgpt.html

Operation Soft Cell: Chinese Hackers Breach Middle East Telecom Providers

Telecommunication providers in the Middle East are the subject of new cyber attacks that commenced in the first quarter of 2023.

The intrusion set has been attributed to a Chinese cyber espionage actor associated with a long-running campaign dubbed Operation Soft Cell based on tooling overlaps. "Once a foothold is established, the attackers conduct a variety of reconnaissance, credential theft, lateral movement, and data exfiltration activities."

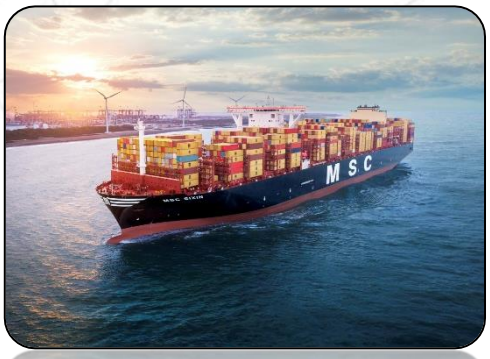
Source:https://thehackernews.com/2023/03/operation-soft-cell-chinese-hackers.html

Hydrochasma: New Threat Actor Targets Shipping Companies and Medical Labs in Asia

Shipping companies and medical laboratories in Asia have been the subject of a suspected espionage campaign carried out by a never-before-seen threat actor dubbed Hydrochasma.

The activity, which has been ongoing since October 2022, "relies exclusively on publicly available and living-off-the-land tools," Symantec, by Broadcom Software, said in a report shared with The Hacker News.

Source:https://thehackernews.com/2023/02/hydrochasma-new-threat-actor-targets.html



New Wi-Fi Protocol Security Flaw Affecting Linux, Android and iOS Devices

A group of academics from Northeastern University and KU Leuven has disclosed a fundamental design flaw in the IEEE 802.11 Wi-Fi protocol standard, impacting a wide range of devices running Linux, FreeBSD, Android, and iOS.

Successful exploitation of the shortcoming could be abused to hijack TCP connections or intercept client and web traffic, researchers Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef said in a paper published this week.

The approach exploits power-save mechanisms in endpoint devices to trick access points into leaking data frames in plaintext, or encrypt them using an all-zero key.

Cisco, in an informational advisory, described the vulnerabilities as an "opportunistic attack and the information gained by the attacker would be of minimal value in a securely configured network."

Source: https://thehackernews.com/2023/03/new-wi-fi-protocol-security-flaw.html

Microsoft Introduces GPT-4 AI-Powered Security Copilot Tool to Empower Defenders

Microsoft on Tuesday unveiled Security Copilot in limited preview, marking its continued quest to embed AI-oriented features in an attempt to offer "end-to-end defense at machine speed and scale."

Powered by OpenAI's GPT-4 generative AI and its own security-specific model, it's billed as a security analysis tool that enables cybersecurity analysts to quickly respond to threats, process signals, and assess risk exposure.Users, for instance, can ask Security Copilot about suspicious user logins over a specific time period, or even employ it to create a PowerPoint presentation outlining an incident and its attack chain. It can also accept files, URLs, and code snippets for analysis.

Source:https://thehackernews.com/2023/03/microsoft-introduces-gpt-4-ai-powered.html