14 APRIL, 2023 ISSUE 1

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Zero-day attacks on iOS: Apple fights back with urgent security patch.

A recent vulnerability has been discovered in the IOSurfaceAccelerator and WebKit components of iPhone and iPad devices, leaving them open to attack by hackers who could potentially steal personal information or damage the device. Apple has released an update that fixes these vulnerabilities, and it is important for users to update their devices as soon as possible to stay safe. However, it is also recommended to exercise caution when clicking on links or opening attachments from unknown sources, and to use reputable antivirus software for extra protection.

A risk-based vulnerability management service from Armoryze can help organizations identify, prioritize and manage vulnerabilities. By taking a proactive approach to vulnerability management, organizations can stay safe from potential cyber threats.

READ MORE »

3CX Supply Chain Attack: What happened?

A recent software supply-chain attack has been reported in which hackers have tampered with the installer for a widely used VoIP application called 3CX to distribute their malicious code. The hackers, allegedly working for the North Korean government, aimed to gain access to a few cryptocurrency companies. 3CX is taking several measures to address the attack, including conducting a comprehensive investigation and working closely with law enforcement and authorities.

The company has also extended their subscriptions by three months, free of charge, as a gesture of appreciation for their customers' patience and support during this difficult time. Users are advised to uninstall the 3CX Electron Desktop Application from all Windows or Mac OS computers, continue with AV scans and EDR solutions, and switch to using the PWA Web Client App rather than the Desktop App.

READ MORE

Genesis Market, a large cybercrime marketplace, shut down.

Genesis Market, an illegal online marketplace that specialized in the sale of stolen credentials associated with email, bank accounts, and social media platforms, has been dismantled in an "unprecedented" law enforcement exercise codenamed Operation Cookie Monster. The major crackdown, involving authorities from 17 countries, culminated in 119 arrests and 208 property searches in 13 nations. Since its inception in March 2018, Genesis Market had become a major hub for criminal activities.

Offering access to data stolen from over 1.5 million compromised computers across the world totalling more than 80 million credentials. The US Department of Justice called Genesis Market one of the "most prolific initial access brokers (IABs) in the cybercrime world

READ MORE

OpenAI, ChatGPT's creator, offers to pay $20,000 for security flaws.

On Tuesday, OpenAI launched a bug bounty program, offering up to $20,000 for early notification on security vulnerabilities discovered by hackers. The move followed the recent patching of account takeover vulnerabilities in ChatGPT, which were being actively exploited. The Microsoft-backed AI firm plans to award bounties for bugs discovered in ChatGPT, APIs, API keys, third-party corporate targets, and assets belonging to OpenAI's research organization. The program will be managed by BugCrowd and the company is keen to discover defects in the ChatGPT chatbot, including ChatGPT Plus, logins, subscriptions, OpenAI-created plugins, and third-party plugins.

The rewards range from $200 for low-severity findings to $20,000 for significant discoveries based on the severity and impact of the reported issues. Last month, OpenAI experienced a data breach, which exposed ChatGPT users' chat data belonging to others, and it also patched serious vulnerabilities in March, which could have allowed hackers to take over accounts and view chat histories. If you are concerned about the security of your web app and API, consider protecting them with Armoryze Web App and API protection solution.

READ MORE

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

CISA warns of 5 actively exploited security flaws.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added five security flaws to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild. Of these, three high-severity flaws in the Veritas Backup Exec Agent software could lead to the execution of privileged commands on the underlying system. Google-owned Mandiant revealed that an affiliate associated with the BlackCat ransomware operation is targeting publicly exposed Veritas Backup Exec installations to gain initial access by leveraging the three bugs.

Another vulnerability added to the list is an information disclosure flaw in Arm Mali GPU Kernel Driver. Here are the 5 current actively exploited vulnerabilities:

- **CVE-2021-27876** (CVSS score: 8.1): Veritas Backup Exec Agent File Access Vulnerability
- **CVE-2021-27877** (CVSS score: 8.2): Veritas Backup Exec Agent Improper Authentication Vulnerability
- **CVE-2021-27878** (CVSS score: 8.8): Veritas Backup Exec Agent Command Execution Vulnerability
- **CVE-2019-1388** (CVSS score: 7.8): a privilege escalation flaw impacting Microsoft Windows Certificate Dialog.
- **CVE-2023-26083** (CVSS score: 5.5): an information disclosure flaw in Arm Mali GPU Kernel Driver

READ MORE »