Scottish
Cyber
Coordination
Centre

Daily threat bulletin

7 October 2024

Vulnerabilities

Apple Releases Critical iOS and iPadOS Updates to Fix VoiceOver Password Vulnerability

The Hacker News - 05 October 2024 11:20

Apple has released iOS and iPadOS updates to address two security issues, one of which could have allowed a user's passwords to be read out aloud by its VoiceOver assistive technology. The vulnerability, tracked as CVE-2024-44204, has been described as a logic problem in the new Passwords app impacting a slew of iPhones and iPads.

WordPress LiteSpeed Cache plugin flaw could allow site takeover

Security Affairs - 05 October 2024 14:48

A high-severity flaw in the WordPress LiteSpeed Cache plugin could allow attackers to execute arbitrary JavaScript code under certain conditions. A high-severity security flaw, tracked as CVE-2024-47374 (CVSS score 7.2), in the LiteSpeed Cache plugin for WordPress could allow attackers to execute arbitrary JavaScript.

Threat actors and malware

Google Pixel 9 supports new security features to mitigate baseband attacks

Security Affairs - 06 October 2024 09:44

Google announced that its Pixel 9 has implemented new security features, and it supports measures to mitigate baseband attacks. Pixel phones are known for their strong security features, particularly in protecting the cellular baseband, which is the processor handling LTE, 4G, and 5G communications.

Microsoft, DOJ Dismantle Russian Hacker Group Star Blizzard

darkreading - 04 October 2024 20:21

The successful disruption of notorious Russian hacker group Star Blizzard's operations arrives one month out from the US presidential election — one of the APT's prime targets.

China-linked group Salt Typhoon hacked US broadband providers and breached wiretap systems

Security Affairs - 06 October 2024 22:04

China-linked APT group Salt Typhoon breached U.S. broadband providers, potentially accessing systems for lawful wiretapping and other data. China-linked APT group Salt Typhoon (also known as FamousSparrow and GhostEmperor) breached U.S. broadband providers, including Verizon, AT&T, and Lumen Technologies, potentially accessing systems for lawful wiretapping and other data.

How Cybercriminals Use Stolen Data to Target Companies — A Deep Dive into the Dark Web

Security Boulevard - 06 October 2024 16:54

The digital world has revolutionized the way we live and work, but it has also opened up a new realm for cybercriminals. The rise of the dark web has provided a breeding ground for hackers and other malicious actors to trade stolen data and launch attacks against companies worldwide.