Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 April 2025

Vulnerabilities

Apple 'AirBorne' flaws can lead to zero-click AirPlay RCE attacks

BleepingComputer - 29 April 2025 14:32

A set of security vulnerabilities in Apple's AirPlay Protocol and AirPlay Software Development Kit (SDK) exposed unpatched third-party and Apple devices to various attacks, including remote code execution. [...]

CISA tags Broadcom Fabric OS, CommVault flaws as exploited in attacks

BleepingComputer - 29 April 2025 11:15

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) is warning of Broadcom Brocade Fabric OS, Commvault web servers, and Qualitia Active! Mail clients vulnerabilities that are actively exploited in attacks. [...]

AirBorne flaws can lead to fully hijack Apple devices

Security Affairs - 30 April 2025 06:36

Vulnerabilities in Apple's AirPlay protocol and SDK exposed Apple and third-party devices to attacks, including remote code execution. Oligo Security found serious flaws, collectively tracked as AirBorne, in Apple's AirPlay protocol and SDK, affecting Apple and third-party devices. Attackers can exploit the vulnerabilities to perform zero-/one-click RCE, bypass ACLs, read local files, steal data, and [...]

U.S. CISA adds SAP NetWeaver flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 30 April 2025 01:05

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds SAP NetWeaver flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SAP NetWeaver flaw, tracked as CVE-2025-31324, to its Known Exploited Vulnerabilities (KEV) catalog. Last week, researchers warned that a zero-day vulnerability, tracked as CVE-2025-31324 (CVSS score of 10/10), in SAP NetWeaver is [...]

Google Threat Intelligence Group (GTIG) tracked 75 actively exploited zero-day flaws in 2024

Security Affairs - 29 April 2025 13:25

Google tracked 75 zero-day flaws exploited in 2024, down from 98 in 2023, according to its Threat Intelligence Group's latest analysis. In 2024, Google tracked 75 exploited zero-day vulnerabilities, down from 98 in 2023 but up from 63 in 2022. The researchers from Google Threat Intelligence Group (GTIG) observed that most targeted are end-user platforms, [...]

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers ramp up scans for leaked Git tokens and secrets

BleepingComputer - 29 April 2025 16:02

Threat actors are intensifying internet-wide scanning for Git configuration files that can reveal sensitive secrets and authentication tokens used to compromise cloud services and source code repositories. [...]

France ties Russian APT28 hackers to 12 cyberattacks on French orgs

BleepingComputer - 29 April 2025 15:57

Today, the French foreign ministry blamed the APT28 hacking group linked to Russia's military intelligence service (GRU) for targeting or breaching a dozen French entities over the last four years. [...]

SentinelOne warns of threat actors targeting its systems and high-value clients

Security Affairs - 29 April 2025 19:49

SentinelOne warns China-linked APT group PurpleHaze attempted reconnaissance on its systems and high-value clients. Cybersecurity firm SentinelOne warns that a China-linked APT group, tracked as PurpleHaze, attempted to conduct reconnaissance on its infrastructure and high-value clients. The activity suggests targeted cyberespionage efforts aimed at gathering information for potential future attacks.