Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 July 2025

Vulnerabilities

Over 1,200 Citrix servers unpatched against critical auth bypass flaw

BleepingComputer - 30 June 2025 08:47

Over 1,200 Citrix NetScaler ADC and NetScaler Gateway appliances exposed online are unpatched against a critical vulnerability believed to be actively exploited, allowing threat actors to bypass authentication by hijacking user sessions. [...]

Airoha Chip Vulns Put Sony, Bose Earbuds & Headphones at Risk

darkreading - 30 June 2025 20:33

The vulnerabilities, which have yet to be published, could allow a threat actor to hijack not only Bluetooth earbuds and headphones but also the devices connected to them.

Threat actors and malware

Microsoft Defender for Office 365 now blocks email bombing attacks

BleepingComputer - 30 June 2025 13:04

Microsoft says its Defender for Office 365 cloud-based email security suite will now automatically detect and block email bombing attacks. [...]

U.S. Agencies Warn of Rising Iranian Cyberattacks on Defense, OT Networks, and Critical Infrastructure

The Hacker News - 30 June 2025 22:59

U.S. cybersecurity and intelligence agencies have issued a joint advisory warning of potential cyber attacks from Iranian state-sponsored or affiliated threat actors.

Millions of Android, iPhone Users Could Be Sending Data to China

Security Magazine - 30 June 2025 12:00

Apple and Google app stores are offering private browsing apps owned by Chinese companies.

Scattered Spider Hacking Spree Continues With Airline Sector Attacks

darkreading - 30 June 2025 22:36

Microsoft has called the hacker collective one of the most dangerous current cyberthreats.