Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

13 June 2025

Vulnerabilities

U.S. CISA adds Wazuh, and WebDAV flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 12 June 2025 10:17

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Wazuh, and WebDAV flaws to its Known Exploited Vulnerabilities catalog.

CISA Releases Cybersecurity Advisory on SimpleHelp RMM Vulnerability

CISA Advisories -

Today, CISA released Cybersecurity Advisory: Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider.

Trend Micro fixes critical vulnerabilities in multiple products

BleepingComputer - 12 June 2025 16:31

Trend Micro has released security updates to address multiple critical-severity remote code execution and authentication bypass vulnerabilities that impact its Apex Central and Endpoint Encryption (TMEE) PolicyServer products.

Palo Alto Networks Patches Series of Vulnerabilities

Infosecurity Magazine - 12 June 2025 14:15

The cybersecurity provider also implemented recent fixes in Chromium that affected its Prisma Access Browser.

Threat actors and malware

Paragon ‘Graphite’ Spyware Linked to Zero-Click Hacks on Newest iPhones

SecurityWeek - 12 June 2025 16:24

Citizen Lab publishes forensic proof that spyware maker Paragon can compromise up-to-date iPhones. Journalists in Europe among victims.

Over 80,000 Microsoft Entra ID Accounts Targeted Using Open-Source TeamFiltration Tool

The Hacker News - 12 June 2025 12:11

Cybersecurity researchers have uncovered a new account takeover (ATO) campaign that leverages an open-source penetration testing framework called TeamFiltration to breach Microsoft Entra ID (formerly Azure Active Directory) user accounts.

Interpol Targets Infostealers: 20,000 IPs Taken Down, 32 Arrested, 216,000 Victims Notified

SecurityWeek - 12 June 2025 09:04

Interpol has announced a crackdown on infostealer malware in Asia as part of an effort called Operation Secure.

UK incidents

‘Major compromise’ at NHS temping arm exposed gaping security holes

The Register - 12 June 2025 11:29

Cybercriminals broke into systems belonging to the UK’s NHS Professionals body in May 2024, stealing its Active Directory database, but the healthcare organisation never publicly disclosed it.