Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

7 July 2025

Vulnerabilities

Critical Sudo bugs expose major Linux distros to local Root exploits

Security Affairs - 04 July 2025 21:04

Critical Sudo flaws let local users gain root access on Linux systems, the vulnerabilities affect major Linux distributions. Cybersecurity researchers disclosed two vulnerabilities in the Sudo command-line utility for Linux and Unix-like operating systems. Local attackers can exploit the vulnerabilities to escalate privileges to root on affected systems.

NightEagle APT Exploits Microsoft Exchange Flaw to Target China's Military and Tech Sectors

The Hacker News - 04 July 2025 19:29

Cybersecurity researchers have shed light on a previously undocumented threat actor called NightEagle (aka APT-Q-95) that has been observed targeting Microsoft Exchange servers as a part of a zero-day exploit chain designed to target government, defense, and technology sectors in China.

Threat actors and malware

Hunters International ransomware gang shuts down and offers free decryption keys to all victims

Security Affairs - 06 July 2025 14:28

Hunters International ransomware gang announced its shutdown, citing unspecified “recent developments” and acknowledging its impact. The ransomware group Hunters International announced on its dark web site that it is shutting down, citing “recent developments” without specifying details.

North Korea-linked threat actors spread macOS NimDoor malware via fake Zoom updates

Security Affairs - 05 July 2025 17:32

North Korea-linked hackers use fake Zoom updates to spread macOS NimDoor malware, targeting crypto firms with stealthy backdoors. North Korea-linked threat actors are targeting Web3 and crypto firms with NimDoor, a rare macOS backdoor disguised as a fake Zoom update. Victims are tricked into installing the malware through phishing links sent via Calendly or Telegram. […]

Mastering Real-Time Cloud Data Governance Amid Evolving Threats and Regulations

Security Boulevard - 04 July 2025 11:09

Real-time data governance provides security and privacy teams with immediate visibility into what is happening, allowing them to stop a problem before it becomes a crisis.

Ransomware: Hunters International Is Not Shutting Down, It’s Rebranding

Infosecurity Magazine - 04 July 2025 12:45

Some admins of Hunters International are now part of the encryption-less cyber extortion group World Leaks