Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 July 2025

Vulnerabilities

CISA warns of hackers exploiting SysAid vulnerabilities in attacks

BleepingComputer - 23 July 2025 10:30

CISA has warned that attackers are actively exploiting two security vulnerabilities in the SysAid IT service management (ITSM) software to hijack administrator accounts.

Sophos fixed two critical Sophos Firewall vulnerabilities

Security Affairs - 23 July 2025 21:23

Sophos has fixed five vulnerabilities (CVE-2025-6704, CVE-2025-7624, CVE-2025-7382, CVE-2024-13974, CVE-2024-13973) in Sophos Firewall that could allow an attacker to remotely execute arbitrary code.

High-Severity Flaws Patched in Chrome, Firefox

SecurityWeek - 23 July 2025 10:58

Fresh security updates for Chrome and Firefox resolve multiple high-severity memory safety vulnerabilities.

Threat actors and malware

NPM package 'is' with 2.8M weekly downloads infected devs with malware

BleepingComputer - 23 July 2025 12:57

The popular NPM package 'is' has been compromised in a supply chain attack that injected backdoor malware, giving attackers full access to compromised devices.

Hackers Deploy Stealth Backdoor in WordPress Mu-Plugins to Maintain Admin Access

The Hacker News - 24 July 2025 11:41

Cybersecurity researchers have uncovered a new stealthy backdoor concealed within the "mu-plugins" directory in WordPress sites to grant threat actors persistent access and allow them to perform arbitrary actions.

Scottish Cyber Coordination Centre

New Coyote Malware Variant Exploits Windows UI Automation to Steal Banking Credentials

The Hacker News - 23 July 2025 19:28

The Windows banking trojan known as Coyote has become the first known malware strain to exploit the Windows accessibility framework called UI Automation (UIA) to harvest sensitive information.

New Crux Ransomware Emerges in Three Attacks This Month

Security Boulevard - 23 July 2025 17:39

A new ransomware variant dubbed “Crux” was detected by Huntress researchers in three attacks this month, with the group favoring RDP for initial access and legitimate processes to make it more difficult to detect it.