Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 September 2025

Vulnerabilities

Critical CVEs in Chaos-Mesh Enable In-Cluster Code Execution

Infosecurity Magazine - 17 September 2025 16:00

A trio of critical vulnerabilities in the Chaos-Mesh platform allow in-cluster attackers to run arbitrary code, even in default configuration

Threat actors and malware

ShinyHunters claims 1.5 billion Salesforce records stolen in Drift hacks

BleepingComputer - 17 September 2025 18:11

The ShinyHunters extortion group claims to have stolen over 1.5 billion Salesforce records from 760 companies using compromised Salesloft Drift OAuth tokens.

SonicWall warns customers to reset credentials after breach

BleepingComputer - 17 September 2025 13:23

SonicWall warned customers today to reset credentials after their firewall configuration backup files were exposed in a security breach that impacted MySonicWall accounts.

From ClickFix to MetaStealer: Dissecting Evolving Threat Actor Techniques

BleepingComputer - 17 September 2025 11:01

ClickFix isn't just back, it's mutating. New variants use fake CAPTCHAs, File Explorer tricks & MSI lures to drop MetaStealer.

Scattered Spider Resurfaces With Financial Sector Attacks Despite Retirement Claims

The Hacker News - 17 September 2025 15:19

Cybersecurity researchers have tied a fresh round of cyber attacks targeting financial services to the notorious cybercrime group known as Scattered Spider, casting doubt on their claims of going "dark.

GOLD SALEM's Warlock operation joins busy ransomware landscape

Threat Research – Sophos News - 17 September 2025 14:00

The emerging group demonstrates competent tradecraft using a familiar ransomware playbook and hints of ingenuity.

Scottish Cyber Coordination Centre

UK incidents

UK telco Colt's recovery from August cyberattack pushes into November

The Register - 17 September 2025 12:45

Pentesters confirm key system is safe but core products remain unavailable Brit telco Colt Technology Services says its recovery from an August cyberattack might not be completed until late November.