Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 August 2025

Vulnerabilities

Passwordstate dev urges users to patch auth bypass vulnerability

BleepingComputer - 28 August 2025 13:16

Click Studios, the company behind the Passwordstate enterprise-grade password manager, has warned customers to patch a high-severity authentication bypass vulnerability as soon as possible.

Researchers Find VS Code Flaw Allowing Attackers to Republish Deleted Extensions Under Same Names

The Hacker News - 28 August 2025 23:40

Cybersecurity researchers have discovered a loophole in the Visual Studio Code Marketplace that allows threat actors to reuse names of previously removed extensions.

Threat actors and malware

NSA, NCSC, and allies detailed TTPs associated with Chinese APT actors targeting critical infrastructure Orgs

Security Affairs - 28 August 2025 11:47

The U.S. National Security Agency (NSA), the UK's National Cyber Security Centre (NCSC), and allies warn Chinese APT actors, linked to Salt Typhoon, are targeting global telecom, government, transport, lodging, and military sectors.

Google warns Salesloft breach impacted some Workspace accounts

BleepingComputer - 28 August 2025 19:09

Google reports that the Salesloft Drift breach is larger than initially thought, warning that attackers also used stolen OAuth tokens to access Google Workspace email accounts in addition to Salesforce data.

Malware devs abuse Anthropic's Claude AI to build ransomware

BleepingComputer - 28 August 2025 14:08

Anthropic's Claude Code large language model has been abused by threat actors who used it in data extortion campaigns and to develop ransomware packages.

Scottish Cyber Coordination Centre

TamperedChef Malware Disguised as Fake PDF Editors Steals Credentials and Cookies

The Hacker News - 29 August 2025 10:47

Cybersecurity researchers have discovered a cybercrime campaign that's using malvertising tricks to direct victims to fraudulent sites to deliver a new information stealer called TamperedChef.

Ransomware Actor Deletes Data and Backups Post-Exfiltration on Azure

Infosecurity Magazine - 28 August 2025 09:05

Microsoft observed Storm-0501 pivot to the victim's cloud environment to exfiltrate data rapidly and prevent the victim's recovery