Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 September 2025

Vulnerabilities

The Critical Failure in Vulnerability Management

darkreading - 08 September 2025 15:00

Organizations are seeking assistance to fix critical vulnerabilities. Solutions that orchestrate and automate network device protection put us on the right path.

SAP S/4HANA Users Urged to Patch Critical Exploited Bug

Infosecurity Magazine - 08 September 2025 09:20

Critical SAP S/4HANA vulnerability CVE-2025-42957 is being exploited in the wild

Threat actors and malware

Surge in networks scans targeting Cisco ASA devices raise concerns

BleepingComputer - 08 September 2025 18:44

Large network scans have been targeting Cisco ASA devices, prompting warnings from cybersecurity researchers that it could indicate an upcoming flaw in the products. [...]

Hackers hijack npm packages with 2 billion weekly downloads in supply chain attack

BleepingComputer - 08 September 2025 13:47

In a supply chain attack, attackers injected malware into NPM packages with over 2.6 billion weekly downloads after compromising a maintainer's account in a phishing attack. [...]

LunaLock Ransomware threatens victims by feeding stolen data to AI models

Security Affairs - 09 September 2025 06:48

LunaLock, a new ransomware gang, introduced a unique cyber extortion technique, threatening to turn stolen art into AI training data. A new ransomware group, named LunaLock, appeared in the threat landscape with a unique cyber extortion technique, threatening to turn stolen art into AI training data.

Hackers breached Salesloft 's GitHub in March, and used stole tokens in a mass attack

Security Affairs - 08 September 2025 20:20

Hackers breached Salesloft's GitHub in March, stole tokens, and used them in a mass attack on several major tech customers. Salesloft revealed that the threat actor UNC6395 breached its GitHub account in March, stealing authentication tokens that were later used in a large-

scale attack against several major tech customers. Salesforce data theft attacks impacted major [...]

Account Profile Scam Targets PayPal Users

Security Magazine - 08 September 2025 09:00

Researchers have discovered a sophisticated, convincing phishing campaign targeting PayPal users.

'MostereRAT' Malware Blends In, Blocks Security Tools

darkreading - 08 September 2025 21:49

A threat actor is using a sophisticated EDR-killing malware tool in a campaign to maintain long-term, persistent access on Windows systems.

CISA sounds alarm over TP-Link wireless routers under attack

The Register - 08 September 2025 12:46

Plus: Google clears up Gmail concerns, NSA drops SBOM bomb, Texas sues PowerSchool, and more Infosec in brief The US Cybersecurity and Infrastructure Security Agency (CISA) has said two flaws in routers made by Chinese networking biz TP-Link are under active attack and need to be fixed – but there's another flaw being exploited as well....

UK related

Cyberattack on Jaguar Land Rover threatens to hit British economic growth

The Record from Recorded Future News - 08 September 2025 19:40