Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 August 2025

Vulnerabilities

Cisco Warns of CVSS 10.0 FMC RADIUS Flaw Allowing Remote Code Execution

The Hacker News - 15 August 2025 13:19

Cisco has released security updates to address a maximum-severity security flaw in Secure Firewall Management Center (FMC) Software that could allow an attacker to execute arbitrary code on affected systems.

OT Networks Targeted in Vulnerability Exploitation

Security Magazine - 15 August 2025 09:00

An Erlang/OTP vulnerability has been exploited in the wild, with a majority of attempts targeting OT environments.

Researcher to release exploit for full auth bypass on FortiWeb

BleepingComputer - 16 August 2025 11:24

A security researcher has released a partial proof of concept exploit for a vulnerability in the FortiWeb web application firewall that allows a remote attacker to bypass authentication.

Plex warns users to patch security vulnerability immediately

BleepingComputer - 15 August 2025 08:41

Plex has notified some of its users to urgently update their media servers due to a recently patched security vulnerability.

Threat actors and malware

Russian Group EncryptHub Exploits MSC EvilTwin Vulnerability to Deploy Fickle Stealer Malware

The Hacker News - 16 August 2025 12:04

Trustwave SpiderLabs said it recently observed an EncryptHub campaign that brings together social engineering and the exploitation of a vulnerability in the Microsoft Management Console (MMC) framework (CVE-2025-26633, aka MSC EvilTwin) to trigger the infection routine via a rogue Microsoft Console (MSC) file.

Scottish Cyber Coordination Centre

ERMAC V3.0 Banking Trojan Source Code Leak Exposes Full Malware Infrastructure

The Hacker News - 16 August 2025 17:11

Cybersecurity researchers have detailed the inner workings of an Android banking trojan called ERMAC 3.0, uncovering serious shortcomings in the operators' infrastructure. The newly uncovered version 3.0 reveals a significant evolution of the malware, expanding its form injection and data theft capabilities to target more than 700 banking, shopping, and cryptocurrency applications

Taiwan Web Servers Breached by UAT-7237 Using Customized Open-Source Hacking Tools

The Hacker News - 15 August 2025 22:50

A Chinese-speaking advanced persistent threat (APT) actor has been observed targeting web infrastructure entities in Taiwan using customized versions of open-sourced tools with an aim to establish long-term access within high-value victim environments.

New Crypto24 Ransomware Attacks Bypass EDR

darkreading - 15 August 2025 19:49

While several cybercrime groups have embraced "EDR killers," researchers say the deep knowledge and technical skills demonstrated by Crypto24 signify a dangerous escalation.

UK incidents

Colt Technology faces multi-day outage after WarLock ransomware attack

Security Affairs - 18 August 2025 00:23

UK-based Colt Technology Services suffered a cyberattack, reportedly caused by WarLock ransomware, resulting in multi-day outages for hosting, porting, Colt Online, and Voice API services.