Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 October 2025

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a critical security flaw impacting Adobe Experience Manager to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. The vulnerability in question is CVE-2025-54253 (CVSS score: 10.0), a maximum-severity misconfiguration bug that could result in arbitrary code execution.

Two CVSS 10.0 Bugs in Red Lion RTUs Could Hand Hackers Full Industrial Control

The Hacker News - 15 October 2025 13:20

Cybersecurity researchers have disclosed two critical security flaws impacting Red Lion Sixnet remote terminal unit (RTU) products that, if successfully exploited, could result in code execution with the highest privileges.

F5 releases BIG-IP patches for stolen security vulnerabilities

BleepingComputer - 15 October 2025 15:01

Cybersecurity company F5 has released security updates to address BIG-IP vulnerabilities stolen in a breach detected on August 9, 2025.

Two New Windows Zero-Days Exploited in the Wild — One Affects Every Version Ever Shipped

The Hacker News - 15 October 2025 15:53

Microsoft on Tuesday released fixes for a whopping 183 security flaws spanning its products, including three vulnerabilities that have come under active exploitation in the wild, as the tech giant officially ended support for its Windows 10 operating system unless the PCs are enrolled in the Extended Security Updates (ESU) program.

High-Severity Vulnerabilities Patched by Fortinet and Ivanti

SecurityWeek - 15 October 2025 08:45

Fortinet and Ivanti have announced their October 2025 Patch Tuesday updates, which patch many vulnerabilities across their products.

Scottish Cyber Coordination Centre

Flaw in Slider Revolution Plugin Exposed 4m WordPress Sites

Infosecurity Magazine - 15 October 2025 16:45

A flaw in the Slider Revolution plugin has exposed millions of WordPress sites to unauthorized file access

200,000 Linux systems from Framework are shipped with signed UEFI components vulnerable to Secure Boot bypass

Security Affairs - 15 October 2025 15:22

Firmware security company Eclypsium warns that about 200,000 Linux systems from Framework are shipped with signed UEFI components vulnerable to Secure Boot bypass, allowing bootkit installation and persistence.

Threat actors and malware

Chinese Threat Group 'Jewelbug' Quietly Infiltrated Russian IT Network for Months

The Hacker News - 15 October 2025 23:58

A threat actor with ties to China has been attributed to a five-month-long intrusion targeting a Russian IT service provider, marking the hacking group's expansion to the country beyond Southeast Asia and South America.

Hackers Target ICTBroadcast Servers via Cookie Exploit to Gain Remote Shell Access

The Hacker News - 15 October 2025 12:46

Cybersecurity researchers have disclosed that a critical security flaw impacting ICTBroadcast, an autodialer software from ICT Innovations, has come under active exploitation in the wild. The vulnerability, assigned the CVE identifier CVE-2025-2611 (CVSS score: 9.3), relates to improper input validation that can result in unauthenticated remote code execution.

Whisper 2FA Behind One Million Phishing Attempts Since July

Infosecurity Magazine - 15 October 2025 16:00

Whisper 2FA is now one of the most active PhaaS tools alongside Tycoon and EvilProxy, responsible for one million attacks since July 2025.

Qilin Ransomware announced new victims

Security Affairs - 15 October 2025 20:42

The following new report by Resecurity will explore the Qilin ransomware-as-a-service (RaaS) operation's reliance on bullet-proof-hosting (BPH) infrastructures, with an emphasis on a network of rogue providers based in different parts of the world.

Scottish Cyber Coordination Centre

UK incidents

Capita to pay £14 million for data breach impacting 6.6 million people

BleepingComputer - 15 October 2025 17:53

The Information Commissioner's Office (ICO) in the UK has fined Capita, a provider of data-driven business process services, £14 million ($18.7 million) for a data breach incident in 2023 that exposed the personal information of 6.6 million people.