Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 July 2025

Vulnerabilities

UK launches vulnerability research program for external experts

BleepingComputer - 14 July 2025 17:21

UK's National Cyber Security Centre (NCSC) has announced a new Vulnerability Research Initiative (VRI) that aims to strengthen relations with external cybersecurity experts. [...]

Gigabyte motherboards vulnerable to UEFI malware bypassing Secure Boot

BleepingComputer - 14 July 2025 13:30

Dozens of Gigabyte motherboard models run on UEFI firmware vulnerable to security issues that allow planting bootkit malware that is invisible to the operating system and can survive reinstalls. [...]

Experts uncover critical flaws in Kigen eSIM technology affecting billions

Security Affairs - 14 July 2025 12:09

Experts devised a new hack targeting Kigen eSIM tech, used in over 2B devices, exposing smartphones and IoT users to serious security risks. Researchers at Security Explorations uncovered a new hacking method exploiting flaws in Kigen's eSIM tech, affecting billions of IoT devices. An eSIM (embedded SIM) is a digital version of a traditional SIM [...]

4 Critical, Known Exploited Vulnerabilities Added to KEV Catalog

Security Magazine - 14 July 2025 10:00

CISA added 4 new vulnerabilities to the Known Exploited Vulnerabilities (KEV) Catalogue, citing evidence of active exploitation.

Google Gemini AI Bug Allows Invisible, Malicious Prompts

darkreading - 14 July 2025 20:13

A prompt-injection vulnerability in the AI assistant allows attackers to create messages that appear to be legitimate Google Security alerts but instead can be used to target users across various Google products with vishing and phishing.

CitrixBleed 2 Flaw Poses Unacceptable Risk: CISA

SecurityWeek - 14 July 2025 15:38

CISA considers the recently disclosed CitrixBleed 2 vulnerability an unacceptable risk and has added it to the KEV catalog.The post CitrixBleed 2 Flaw Poses Unacceptable Risk: CISA appeared first on SecurityWeek.

Scottish Cyber Coordination Centre

Exploited Wing file transfer bug risks 'total server compromise,' CISA warns

The Record from Recorded Future News - 14 July 2025 21:57

Threat actors and malware

New PHP-Based Interlock RAT Variant Uses FileFix Delivery Mechanism to Target Multiple Industries

The Hacker News - 14 July 2025 23:22

Threat actors behind the Interlock ransomware group have unleashed a new PHP variant of its bespoke remote access trojan (RAT) as part of a widespread campaign using a variant of ClickFix called FileFix."Since May 2025, activity related to the Interlock RAT has been observed in connection with the LandUpdate808 (aka KongTuke) web-inject threat clusters.

Hackers Inject Malware Into Gravity Forms WordPress Plugin

SecurityWeek - 14 July 2025 10:31

Two Gravity Forms WordPress plugin versions available on the official download page were injected with malware in a supply chain attack.The post Hackers Inject Malware Into Gravity Forms WordPress Plugin appeared first on SecurityWeek.

UK related

UK launches vulnerability research program for external experts

BleepingComputer - 14 July 2025 17:21

UK's National Cyber Security Centre (NCSC) has announced a new Vulnerability Research Initiative (VRI) that aims to strengthen relations with external cybersecurity experts. [...]