Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 August 2025

Vulnerabilities

Over 800 N-able servers left unpatched against critical flaws

BleepingComputer - 18 August 2025 13:06

Over 800 N-able N-central servers remain unpatched against a pair of critical security vulnerabilities tagged as actively exploited last week. [...]

Xerox fixed path traversal and XXE bugs in FreeFlow Core

Security Affairs - 18 August 2025 08:08

Xerox patched two serious flaws in FreeFlow Core, path traversal and XXE injection, that allowed unauthenticated remote code execution. Xerox addressed two serious flaws, respectively tracked as CVE-2025-8355 and CVE-2025-8356, in FreeFlow Core.

Microsoft Windows Vulnerability Exploited to Deploy PipeMagic RansomExx Malware

The Hacker News - 18 August 2025 22:33

Cybersecurity researchers have lifted the lid on the threat actors' exploitation of a now-patched security flaw in Microsoft Windows to deploy the PipeMagic malware in RansomExx ransomware attacks.

Malicious PyPI and npm Packages Discovered Exploiting Dependencies in Supply Chain Attacks

The Hacker News - 18 August 2025 17:26

Cybersecurity researchers have discovered a malicious package in the Python Package Index (PyPI) repository that introduces malicious behavior through a dependency that allows it to establish persistence and achieve code execution.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-54948 Trend Micro Apex One OS Command Injection Vulnerability.

Threat actors and malware

ERMAC Android malware source code leak exposes banking trojan infrastructure

BleepingComputer - 18 August 2025 15:12

The source code for version 3 of the ERMAC Android banking trojan has been leaked online, exposing the internals of the malware-as-a-service platform and the operator's infrastructure. [...]

Noodlophile Malware Campaign Expands Global Reach with Copyright Phishing Lures

The Hacker News - 19 August 2025 01:54

The threat actors behind the Noodlophile malware are leveraging spear-phishing emails and updated delivery mechanisms to deploy the information stealer in attacks aimed at enterprises located in the U.S., Europe, Baltic countries, and the Asia-Pacific (APAC) region.

Novel 5G Attack Bypasses Need for Malicious Base Station

SecurityWeek - 18 August 2025 16:30

Researchers detailed a new 5G attack named Sni5Gect that can allow attackers to sniff traffic and cause disruption.

Workday Data Breach Bears Signs of Widespread Salesforce Hack

SecurityWeek - 18 August 2025 12:59

Workday appears to have joined the list of major companies that had their Salesforce instances targeted by hackers.

UK related

UK sentences "serial hacker" of 3,000 sites to 20 months in prison

BleepingComputer - 18 August 2025 13:36

A 26-year old in the UK who claimed to have hacked thousands of websites was sentenced to 20 months in prison after pleading guilty earlier this year. [...]

Colt Customers Face Prolonged Outages After Major Cyber Incident

Infosecurity Magazine - 18 August 2025 11:30

The Warlock ransomware gang has taken credit for the cyber-attack after the UK telco giant publicly confirmed an incident on August 14