Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 August 2026

Vulnerabilities

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA - 18 August 2026 12:00

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-33824 Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability
CVE-2026-55040 Microsoft SharePoint Weak Authentication Vulnerability
CVE-2026-59310 Broadcom VMware vCenter Path Traversal Vulnerability
CVE-2026-65400 Apple macOS Improper Authentication Vulnerability

CISA: Windows Task Host flaw now exploited by ransomware gangs

Bleeping Computer - 18 August 2026 06:32

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has confirmed that ransomware gangs are also exploiting a high-severity Windows Task Host vulnerability that was flagged as actively exploited in April.

Critical MLflow SSRF Vulnerability Exploited by Hackers in the Wild

Cyber Security News - 18 August 2026 16:52

Threat actors are actively exploiting a critical, unauthenticated server-side request forgery (SSRF) vulnerability in MLflow, the popular open-source platform widely used by data engineering and machine learning teams to track experiments, package code, and deploy models.

GitLab Patches Critical Unauthenticated GraphQL Vulnerability

Security Affairs - 18 August 2026 08:44

GitLab pushed out an emergency patch this week to address a critical flaw, tracked as CVE-2026-19478 (CVSS score of 9.4), that could let an attacker with zero credentials remotely modify or delete public projects and user data.

300,000 WordPress Sites Potentially Exposed to Hacking Due to Form Plugin Flaw

Security Week - 18 August 2026 10:48

Tracked as CVE-2026-15748, the arbitrary file upload bug allows unauthenticated attackers to upload executable files.

Scottish Cyber Coordination Centre

Microsoft Copilot Personal Flaws Could Let One Click Exfiltrate Data From Connected Apps

The Hacker News - 18 August 2026 23:17

Varonis Threat Labs has disclosed three vulnerabilities in Microsoft Copilot Personal that it said could allow a single click on a crafted link to silently pull data from connected apps and other information available to the victim's Copilot session.

Threat actors and malware

Clop created custom web shell for Windchill data theft attacks

Bleeping Computer - 18 August 2026 13:29

A custom Java web shell likely linked to the Clop ransomware gang was designed specifically for PTC Windchill and FlexPLM servers, with built-in features to decrypt credentials, enumerate file repositories, and steal files.

New Mirai-Based Evooo1Bot Botnet Targets Linux Devices

Security Affairs - 18 August 2026 07:18

Evooo1Bot is a Mirai-based Linux botnet that hijacks routers and IoT devices for DDoS attacks, credential theft and criminal proxy services. Fortinet's FortiGuard Labs disclosed Evooo1Bot in mid-August, a previously undocumented Linux botnet that's been active since July 2026.

One Attacker Has Scraped Both Salesforce and ServiceNow Portals Since 2025

The Hacker News - 18 August 2026 17:00

A single piece of infrastructure has been pulling records out of Salesforce and ServiceNow customer portals across multiple industries for more than a year, according to research published this week by agent security platform Reco.

Projextor Shows How Malware Can Hide Behind Trusted Electron Executables

Cyber Security News - 18 August 2026 15:34

Projextor is a malware campaign that turns ordinary-looking desktop tools into a doorway for hidden code. Its operators package it inside working document converters, meal planners and recipe applications, so victims receive a program that appears useful from the first click.

Medusa ransomware tallies hundreds of new victims, says updated advisory on group's tactics

CyberScoop - 18 August 2026 17:18

The updated warning from the FBI, CISA and HHS draws on a year's worth of investigations to detail how the group gains initial access and what it does afterward.