Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 May 2025

Vulnerabilities

Mozilla fixes Firefox zero-days exploited at hacking contest

BleepingComputer - 19 May 2025 11:10

Mozilla released emergency security updates to address two Firefox zero-day vulnerabilities demonstrated in the recent Pwn2Own Berlin 2025 hacking competition. [...]

Security Leaders Discuss the New EU Vulnerability Database

Security Magazine - 19 May 2025 09:00

Security leaders share their thoughts on the new EU vulnerability database.

RCE Vulnerability Found in RomethemeKit For Elementor Plugin

Infosecurity Magazine - 19 May 2025 16:00

RomethemeKit for Elementor has released a patch addressing an RCE vulnerability exposing 30,000 sites

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2025-4427 Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability; CVE-2025-4428 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability; CVE-2024-11182 MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability; CVE-2025-27920 Srimax Output Messenger Directory Traversal Vulnerability; CVE-2024-27443 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability; CVE-2023-38950 ZKTeco BioTime Path Traversal Vulnerability.

Threat actors and malware

Fake KeePass password manager leads to ESXi ransomware attack

BleepingComputer - 19 May 2025 18:17

Threat actors have been distributing trojanized versions of the KeePass password manager for at least eight months to install Cobalt Strike beacons, steal credentials, and ultimately, deploy ransomware on the breached network. [...]

Arla Foods confirms cyberattack disrupts production, causes delays

BleepingComputer - 19 May 2025 14:53

Arla Foods has confirmed to BleepingComputer that it was targeted by a cyberattack that has disrupted its production operations. [...]

RVTools Official Site Hacked to Deliver Bumblebee Malware via Trojanized Installer

The Hacker News - 19 May 2025 22:18

The official site for RVTools has been hacked to serve a compromised installer for the popular VMware environment reporting utility."Robware.net and RVTools.com are currently offline. We are working expeditiously to restore service and appreciate your patience," the company said in a statement posted on its website.

ADR Blocks Spike in Cyber Attacks and Sharp Rise in Path Traversal Attacks | April Attack Data | Contrast Security

Security Boulevard - 19 May 2025 19:05

Customers using Application Detection and Response (ADR) technology blocked a remarkable number of attacks over the past month. For the second time since we began writing this monthly report, we've seen a massive escalation of attacks against a small number of applications, and all of the attacks were blocked.

UK related

O2 UK patches bug leaking mobile user location from call metadata

BleepingComputer - 19 May 2025 16:20

A flaw in O2 UK's implementation of VoLTE and WiFi Calling technologies could allow anyone to expose the general location of a person and other identifiers by calling the target. [...]

UK Legal Aid Agency confirms applicant data stolen in data breach

BleepingComputer - 19 May 2025 12:10

The United Kingdom's Legal Aid Agency (LAA) has confirmed that a recent cyberattack is more serious than first believed, with hackers stealing a large trove of sensitive applicant data in a data breach. [...]