Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 October 2025

Vulnerabilities

Clop exploited Oracle zero-day for data theft since early August

BleepingComputer - 07 October 2025 14:27

The Clop ransomware gang has been exploiting a critical Oracle E-Business Suite (EBS) zero-day bug in data theft attacks since at least early August, according to cybersecurity company CrowdStrike.

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-2025-27915 Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability

GoAnywhere MFT zero-day used by Storm-1175 in Medusa ransomware campaigns

Security Affairs - 07 October 2025 20:23

A cybercrime group, tracked as Storm-1175, has been actively exploiting a maximum severity GoAnywhere MFT vulnerability (CVE-2025-10035) in Medusa ransomware attacks for nearly a month.

13-Year-Old Redis Flaw Exposed: CVSS 10.0 Vulnerability Lets Attackers Run Code Remotely

The Hacker News - 07 October 2025 15:03

Redis has disclosed details of a maximum-severity security flaw in its in-memory database software that could result in remote code execution under certain circumstances .

Google's New AI Doesn't Just Find Vulnerabilities — It Rewrites Code to Patch Them

The Hacker News - 07 October 2025 21:48

Google's DeepMind division on Monday announced an artificial intelligence (AI)-powered agent called CodeMender that automatically detects, patches, and rewrites vulnerable code to prevent future exploits.

Scottish Cyber Coordination Centre

Threat actors and malware

Salesforce refuses to pay ransom over widespread data theft attacks

BleepingComputer - 07 October 2025 21:17

Salesforce has confirmed that it will not negotiate with or pay a ransom to the threat actors behind a massive wave of data theft attacks that impacted the company's customers this year.

Google won't fix new ASCII smuggling attack in Gemini

BleepingComputer - 07 October 2025 17:35

Google has decided not to fix a new ASCII smuggling attack in Gemini that could be used to trick the AI assistant into providing users with fake information, alter the model's behavior, and silently poison its data.

BatShadow Group Uses New Go-Based 'Vampire Bot' Malware to Hunt Job Seekers

The Hacker News - 07 October 2025 23:34

A Vietnamese threat actor named BatShadow has been attributed to a new campaign that leverages social engineering tactics to deceive job seekers and digital marketing professionals to deliver a previously undocumented malware called Vampire Bot.

Qilin Ransomware Gang Claims Asahi Cyber-Attack

Infosecurity Magazine - 07 October 2025 18:15

The Qilin group claims to have stolen sensitive personal and proprietary data from the Brewer

UK incidents

Jaguar Land Rover to restart production following cyberattack

The Record from Recorded Future News - 07 October 2025 12:55

Jaguar Land Rover (JLR) announced on Tuesday it will begin the phased restart of its manufacturing operations following a cyberattack that completely halted global production last month.