Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 November 2025

Vulnerabilities

CISA warns Oracle Identity Manager RCE flaw is being actively exploited

BleepingComputer - 21 November 2025 19:50

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) is warning government agencies to patch an Oracle Identity Manager tracked as CVE-2025-61757 that has been exploited in attacks, potentially as a zero-day.

Grafana Patches CVSS 10.0 SCIM Flaw Enabling Impersonation and Privilege Escalation

The Hacker News - 21 November 2025 22:10

The vulnerability, tracked as CVE-2025-41115, carries a CVSS score of 10.0. It resides in the System for Cross-domain Identity Management (SCIM) component that allows automated user provisioning and management.

SolarWinds addressed three critical flaws in Serv-U

Security Affairs - 21 November 2025 15:08

SolarWinds patched three critical vulnerabilities in its Serv-U file transfer solution that could allow remote code execution.

SonicWall flags SSLVPN flaw allowing firewall crashes

Security Affairs - 23 November 2025 11:34

A new high-severity SonicOS SSLVPN flaw, tracked as CVE-2025-40601 (CVSS score of 7.5), allows attackers to crash SonicWall Gen7 and Gen8 firewalls.

Threat actors and malware

BadAudio malware: how APT24 scaled its cyberespionage through supply chain attacks

Security Affairs - 22 November 2025 18:11

China-linked group APT24 used supply-chain attacks and multiple techniques over three years to deploy the BadAudio downloader and additional malware payloads, Google Threat Intelligence Group (GTIG) warns.

Scottish Cyber Coordination Centre

China-Linked APT31 Launches Stealthy Cyberattacks on Russian IT Using Cloud Services

The Hacker News - 22 November 2025 21:49

The China-linked advanced persistent threat (APT) group known as APT31 has been attributed to cyber attacks targeting the Russian information technology (IT) sector between 2024 and 2025 while staying undetected for extended periods of time.

Matrix Push C2 Uses Browser Notifications for Fileless, Cross-Platform Phishing Attacks

The Hacker News - 22 November 2025 13:17

Bad actors are leveraging browser notifications as a vector for phishing attacks to distribute malicious links by means of a new command-and-control (C2) platform called Matrix Push C2.

Salesforce Instances Hacked via Gainsight Integrations

SecurityWeek - 21 November 2025 10:38

The infamous ShinyHunters hackers have targeted customer-managed Gainsight-published applications to steal data from Salesforce instances.

CrowdStrike denies breach after insider sent internal screenshots to hackers

Security Affairs - 21 November 2025 22:31

CrowdStrike says an insider shared internal screenshots with hackers but confirms no system breach and no customer data exposure. CrowdStrike said an insider shared internal system screenshots with hackers, after Scattered Lapsus$ Hunters leaked them on Telegram.

Piecing Together the Puzzle: A Qilin Ransomware Investigation

BleepingComputer - 22 November 2025 09:45

Huntress analysts reconstructed a Qilin ransomware attack from a single endpoint, using limited logs to reveal rogue ScreenConnect access, failed infostealer attempts, and the ransomware execution path.

UK incidents

‘Scattered Spider’ teens plead not guilty to UK transport hack

BleepingComputer - 21 November 2025 11:41

Two British teenagers have denied charges related to an investigation into the breach of Transport for London (TfL) in August 2024, which caused millions of pounds in damage and exposed customer data.