Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 April 2025

Vulnerabilities

Ivanti Releases Security Updates for Connect Secure, Policy Secure & ZTA Gateways Vulnerability (CVE-2025-22457)

CISA Advisories -

Ivanti released security updates to address vulnerabilities (CVE-2025-22457) in Ivanti Connect Secure, Policy Secure & ZTA Gateways. A cyber threat actor could exploit CVE-2025-22457 to take control of an affected system.
CISA has also added CVE-2025-22457 to its Known Exploited Vulnerabilities Catalog.

Critical flaw in Apache Parquet's Java Library allows remote code execution

Security Affairs - 04 April 2025 11:00

Experts warn of a critical vulnerability impacting Apache Parquet's Java Library that could allow remote code execution. Apache Parquet's Java Library is a software library for reading and writing Parquet files in the Java programming language.

WinRAR flaw bypasses Windows Mark of the Web security alerts

BleepingComputer - 05 April 2025 11:14

A vulnerability in the WinRAR file archiver solution could be exploited to bypass the Mark of the Web (MotW) security warning and execute arbitrary code on a Windows machine.

Microsoft Credits EncryptHub, Hacker Behind 618+ Breaches, for Disclosing Windows Flaws

The Hacker News - 05 April 2025 22:20

A likely lone wolf actor behind the EncryptHub persona was acknowledged by Microsoft for discovering and reporting two security flaws in Windows last month, painting a picture of a "conflicted" individual straddling a legitimate career in cybersecurity and pursuing cybercrime.

Threat actors and malware

Oracle privately notifies Cloud data breach to customers

Security Affairs - 06 April 2025 21:33

Oracle confirms a data breach and started informing customers while downplaying the impact of the incident.

CISA Releases Malware Analysis Report on RESURGE Malware Associated with Ivanti Connect Secure

CISA Advisories -

CISA has published a Malware Analysis Report (MAR) with analysis and associated detection signatures on a new malware variant CISA has identified as RESURGE. RESURGE contains capabilities of the SPAWNCHIMERA malware variant, including surviving reboots; however, RESURGE contains distinctive commands that alter its behavior.

Fast Flux: A National Security Threat

CISA Advisories -

Many networks have a gap in their defenses for detecting and blocking a malicious technique known as “fast flux.” This technique poses a significant threat to national security, enabling malicious cyber actors to consistently evade detection. Malicious cyber actors, including cybercriminals and nation-state actors, use fast flux to obfuscate the locations of malicious servers by rapidly changing Domain Name System (DNS) records.

North Korean Hackers Deploy BeaverTail Malware via 11 Malicious npm Packages

The Hacker News - 05 April 2025 20:53

The North Korean threat actors behind the ongoing Contagious Interview campaign are spreading their tentacles on the npm ecosystem by publishing more malicious packages that deliver the BeaverTail malware, as well as a new remote access trojan (RAT) loader.

Medusa Rides Momentum From Ransomware-as-a-Service Pivot

darkreading - 04 April 2025 15:37

Shifting to a RaaS business model has accelerated the group’s growth, and targeting critical industries like healthcare, legal, and manufacturing hasn’t hurt either.

Europcar GitLab breach exposes data of up to 200,000 customers

BleepingComputer - 04 April 2025 11:07

A hacker breached the GitLab repositories of multinational car-rental company Europcar Mobility Group and stole source code for Android and iOS applications, as well as some personal information belonging to up to 200,000 users.

UK Related

Alan Turing Institute: UK can’t handle a fight against AI-enabled crims

The Register - 04 April 2025 09:30

The National Crime Agency (NCA) will “closely examine” the recommendations made by the Alan Turing Institute after it claimed the UK was ill-equipped to tackle AI-enabled crime.