Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 April 2025

Vulnerabilities

China-linked group UNC5221 exploited Ivanti Connect Secure zero-day since mid-March

Security Affairs - 03 April 2025 20:37

Ivanti released security updates to address a critical Connect Secure remote code execution vulnerability tracked as CVE-2025-22457. The vulnerability has been exploited by a China-linked threat actor since at least mid-March 2025.

Max severity RCE flaw discovered in widely used Apache Parquet

BleepingComputer - 03 April 2025 18:29

A maximum severity remote code execution (RCE) vulnerability has been discovered impacting all versions of Apache Parquet up to and including 1.15.0.

Two CVEs, One Critical Flaw: Inside the CrushFTP Vulnerability Controversy

SecurityWeek - 03 April 2025 11:30

Two CVEs now exist for an actively exploited CrushFTP vulnerability and much of the security industry is using the 'wrong one'.

Google Patches Quick Share Vulnerability Enabling Silent File Transfers Without Consent

The Hacker News - 03 April 2025 14:51

Cybersecurity researchers have disclosed details of a new vulnerability impacting Google's Quick Share data transfer utility for Windows that could be exploited to achieve a denial-of-service (DoS) or send arbitrary files to a target's device without their approval.

Vulnerabilities Expose Cisco Meraki and ECE Products to DoS Attacks

SecurityWeek - 03 April 2025 11:00

Cisco fixes two high-severity denial-of-service vulnerabilities in Meraki devices and Enterprise Chat and Email.

Halo ITSM Vulnerability Exposed Organizations to Remote Hacking

SecurityWeek - 03 April 2025 16:45

An unauthenticated SQL injection vulnerability in Halo ITSM could have been exploited to read, modify, or insert data.

Scottish Cyber Coordination Centre

Threat actors and malware

Oracle privately confirms Cloud breach to customers

BleepingComputer - 03 April 2025 12:26

Oracle has finally acknowledged to some customers that attackers have stolen old client credentials after breaching a “legacy environment” last used in 2017.

CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware

The Hacker News - 04 April 2025 11:24

The Computer Emergency Response Team of Ukraine (CERT-UA) has revealed that no less than three cyber attacks were recorded against state administration bodies and critical infrastructure facilities in the country with an aim to steal sensitive data.

Hunters International shifts from ransomware to pure data extortion

BleepingComputer - 03 April 2025 18:06

The Hunters International Ransomware-as-a-Service (RaaS) operation is shutting down and rebranding with plans to switch to data theft and extortion-only attacks.