Scottish Cyber Coordination Centre

Daily threat bulletin

24 May 2024

Vulnerabilities

Ransomware Attacks Exploit VMware ESXi Vulnerabilities in Alarming Pattern

The Hacker News - 23 May 2024 23:33

Ransomware attacks targeting VMware ESXi infrastructure follow an established pattern regardless of the file-encrypting malware deployed, new findings show."Virtualization platforms are a core component of organizational IT infrastructure, yet they often suffer from inherent misconfigurations and vulnerabilities, making them a lucrative and highly effective target for threat actors to abuse."

CISA Warns of Actively Exploited Apache Flink Security Vulnerability

The Hacker News - 23 May 2024 23:14

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a security flaw impacting Apache Flink, an open-source, unified stream-processing and batch-processing framework, to the Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

NVD Leaves Exploited Vulnerabilities Unchecked

Infosecurity Magazine - 23 May 2024 14:00

Over half of CISA's known exploited vulnerabilities disclosed since February 2024 have not yet been analyzed by NIST's National Vulnerability Database.

Critical SQL Injection flaws impact Ivanti Endpoint Manager (EPM)

Security Affairs - 23 May 2024 11:49

Ivanti addressed multiple flaws in the Endpoint Manager (EPM), including remote code execution vulnerabilities. Ivanti this week rolled out security patches to address multiple critical vulnerabilities in the Endpoint Manager (EPM). A remote attacker can exploit the flaws to gain code execution under certain conditions.

Threat actors and malware

Chinese actor 'Unfading Sea Haze' remained undetected for five years

Security Affairs - 23 May 2024 09:55

A previously unknown China-linked threat actor dubbed 'Unfading Sea Haze' has been targeting military and government entities since 2018. Bitdefender researchers discovered a previously unknown China-linked threat actor dubbed 'Unfading Sea Haze' that has been targeting military and government entities since 2018. The threat group focuses on entities in countries in the South China Sea, […]

Inside Operation Diplomatic Specter: Chinese APT Group's Stealthy Tactics Exposed

The Hacker News - 23 May 2024 17:44

Governmental entities in the Middle East, Africa, and Asia are the target of a Chinese advanced persistent threat (APT) group as part of an ongoing cyber espionage campaign dubbed Operation Diplomatic Specter since at least late 2022."An analysis of this threat actor's activity reveals long-term espionage operations against at least seven governmental entities."

Casino cyberattacks put a bullseye on Scattered Spider – and the FBI is closing in

The Register - 23 May 2024 21:16

Mandiant CTO chats to The Reg about the looming fate of this ransomware crew. The cyberattacks against Las Vegas casinos over the summer put a big target on the backs of prime suspects Scattered Spider, according to Mandiant CTO Charles Carmakal.

Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report

SecurityWeek - 23 May 2024 12:00

Attackers are getting more sophisticated, better armed, and faster. Nothing in Rapid7's 2024 Attack Intelligence Report suggests that this will change. The post Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report appeared first on SecurityWeek.

National Records of Scotland Data Breached in NHS Cyber-Attack

Infosecurity Magazine - 23 May 2024 12:02

National Records of Scotland said sensitive personal data it holds was part of information stolen and published online by ransomware attackers from NHS Dumfries and Galloway.