Scottish Cyber Coordination Centre

Daily threat bulletin

26 July 2024

Vulnerabilities

Critical ServiceNow RCE flaws actively exploited to steal credentials

BleepingComputer - 25 July 2024 17:58

Threat actors are chaining together ServiceNow flaws using publicly available exploits to breach government agencies and private firms in data theft attacks.

Progress warns of critical RCE bug in Telerik Report Server

BleepingComputer - 25 July 2024 12:46

Progress Software has warned customers to patch a critical remote code execution security flaw in the Telerik Report Server that can be used to compromise vulnerable devices.

Researchers Reveal ConfusedFunction Vulnerability in Google Cloud Platform

The Hacker News - 25 July 2024 14:59

Cybersecurity researchers have disclosed a privilege escalation vulnerability impacting Google Cloud Platform's Cloud Functions service that an attacker could exploit to access other services and sensitive data in an unauthorized manner.

BIND Updates Resolve High-Severity DoS Vulnerabilities

SecurityWeek - 25 July 2024 14:05

The latest BIND security updates address remotely exploitable vulnerabilities leading to denial-of-service.

Nvidia Patches High-Severity Vulnerabilities in AI, Networking Products

SecurityWeek - 25 July 2024 08:35

Nvidia has patched high-severity vulnerabilities in its Jetson, Mellanox OS, OnyX, Skyway, and MetroX products.

Threat actors and malware

PKfail Secure Boot bypass lets attackers install UEFI malware

BleepingComputer - 25 July 2024 18:42

Hundreds of UEFI products from 10 vendors are susceptible to compromise due to a critical firmware supply-chain issue known as PKfail, which allows attackers to bypass Secure Boot and install malware.

Beware of fake CrowdStrike domains pumping out Lumma infostealing malware

The Register - 25 July 2024 23:30

PSA: Only accept updates via official channels … ironically enough CrowdStrike is the latest lure being used to trick Windows users into downloading and running the notorious Lumma infostealing malware, according to the security shop's threat intel team, which spotted the scam just days after the Falcon sensor update fiasco.

Mandiant Shines Spotlight on APT45 Behind North Korea's Digital Military Machine

SecurityWeek - 25 July 2024 11:00

A fresh Mandiant report documents North Korea's APT45 as a distinct hacking team conducting cyberespionage and ransomware operations.

Malware Attacks Surge 30% in First Half of 2024

Infosecurity Magazine - 25 July 2024 10:15

SonicWall observed a surge in malware attacks in H1 2024, with strains becoming more adept at defense evasion