Scottish Cyber Coordination Centre

Daily threat bulletin

9 May 2024

Vulnerabilities

New BIG-IP Next Central Manager bugs allow device takeover

BleepingComputer - 08 May 2024 16:52

F5 has fixed two high-severity BIG-IP Next Central Manager vulnerabilities, which can be exploited to gain admin control and create rogue accounts on any managed assets. [...]

LiteSpeed Cache WordPress plugin actively exploited in the wild

Security Affairs - 08 May 2024 12:48

Threat actors are exploiting a high-severity vulnerability in the LiteSpeed Cache plugin for WordPress to take over web sites. WPScan researchers reported that threat actors are exploiting a high-severity vulnerability in LiteSpeed Cache plugin for WordPress. LiteSpeed Cache for WordPress (LSCWP) is an all-in-one site acceleration plugin, featuring an exclusive server-level cache and a collection [...]

Android Update Patches Critical Vulnerability

SecurityWeek - 08 May 2024 12:26

Android's May 2024 security update patches 38 vulnerabilities, including a critical bug in the System component.The post Android Update Patches Critical Vulnerability appeared first on SecurityWeek.

RSAC: CISA Launches Vulnrichment Program to Address NVD Challenges

Infosecurity Magazine - 08 May 2024 19:00

CISA launched a new software vulnerability enrichment program to fill the gap left by NIST's National Vulnerability Database backlog

Threat actors and malware

New Spectre-Style 'Pathfinder' Attack Targets Intel CPU, Leak Encryption Keys and Data

The Hacker News - 08 May 2024 20:47

Researchers have discovered two novel attack methods targeting high-performance Intel CPUs that could be exploited to stage a key recovery attack against the Advanced Encryption Standard (AES) algorithm.The techniques have been collectively dubbed Pathfinder by a group of academics from the University of California San Diego, Purdue University, UNC Chapel

Scottish Cyber Coordination Centre

Hijack Loader Malware Employs Process Hollowing, UAC Bypass in Latest Version

The Hacker News - 08 May 2024 17:28

A newer version of a malware loader called Hijack Loader has been observed incorporating an updated set of anti-analysis techniques to fly under the radar."These enhancements aim to increase the malware's stealthiness, thereby remaining undetected for longer periods of time," Zscaler ThreatLabz researcher Muhammed Irfan V A said in a technical report."Hijack

LockBit gang claimed responsibility for the attack on City of Wichita

Security Affairs - 08 May 2024 20:51

The LockBit ransomware group has added the City of Wichita to its Tor leak site and threatened to publish stolen data. Last week, the City of Wichita, Kansas, was the victim of a ransomware attack and shut down its network to contain the threat. Wichita is the most populous city in the U.S. state of [...]