Scottish Cyber Coordination Centre

Daily threat bulletin

31 May 2024

Vulnerabilities

CISA adds Check Point Quantum Security Gateways and Linux Kernel flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 30 May 2024 21:08

CISA adds Check Point Quantum Security Gateways and Linux Kernel flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog: The vulnerability CVE-2024-24919 is a Quantum Gateway information disclosure issue.

RedTail Crypto-Mining Malware Exploiting Palo Alto Networks Firewall Vulnerability

The Hacker News - 30 May 2024 20:54

The threat actors behind the RedTail cryptocurrency mining malware have added a recently disclosed security flaw impacting Palo Alto Networks firewalls to its exploit arsenal.

Researchers Uncover Active Exploitation of WordPress Plugin Vulnerabilities

The Hacker News - 30 May 2024 20:19

Cybersecurity researchers have warned that multiple high-severity security vulnerabilities in WordPress plugins are being actively exploited by threat actors to create rogue administrator accounts for follow-on exploitation.

NIST Getting Outside Help for National Vulnerability Database

SecurityWeek - 30 May 2024 15:21

NIST is receiving support to get the NVD and CVE processing back on track within the next few months. The post NIST Getting Outside Help for National Vulnerability Database appeared first on SecurityWeek.

Threat actors and malware

Pirated Microsoft Office delivers malware cocktail on systems

BleepingComputer - 30 May 2024 17:53

Cybercriminals are distributing a malware cocktail through cracked versions of Microsoft Office promoted on torrent sites. [...]

FlyingYeti Exploits WinRAR Vulnerability to Deliver COOKBOX Malware in Ukraine

The Hacker News - 30 May 2024 23:07

Cloudflare on Thursday said it took steps to disrupt a month-long phishing campaign orchestrated by a Russia-aligned threat actor called FlyingYeti targeting Ukraine.

Cyber Espionage Alert: LilacSquid Targets IT, Energy, and Pharma Sectors

The Hacker News - 30 May 2024 21:56

A previously undocumented cyber espionage-focused threat actor named LilacSquid has been linked to targeted attacks spanning various sectors in the United States (U.S.), Europe, and Asia as part of a data theft campaign since at least 2021.

Europol-Led Operation Endgame Hits Botnet, Ransomware Networks

Infosecurity Magazine - 30 May 2024 17:15

The operation targeted several significant malware droppers, including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee.

The Ticketmaster breach, what you need to know

Malwarebytes - 30 May 2024 11:26

A database has been put up for sale that allegedly contains the data of 560 million Ticketmaster users. But is it real?

BBC suffers data breach impacting current, former employees

BleepingComputer - 30 May 2024 11:02

The BBC has disclosed a data security incident that occurred on May 21, involving unauthorized access to files hosted on a cloud-based service, compromising the personal information of BBC Pension Scheme members. [...]