Scottish Cyber Coordination Centre

Daily threat bulletin

28 May 2024

Vulnerabilities

TP-Link fixes critical RCE bug in popular C5400X gaming router

BleepingComputer - 27 May 2024 16:11

The TP-Link Archer C5400X gaming router is vulnerable to security flaws that could enable an unauthenticated, remote attacker to execute commands on the device. [...]

A high-severity vulnerability affects Cisco Firepower Management Center

Security Affairs - 27 May 2024 07:58

Cisco addressed a SQL injection vulnerability in the web-based management interface of the Firepower Management Center (FMC) Software. Cisco addressed a vulnerability, tracked as CVE-2024-20360 (CVSS score 8.8), in the web-based management interface of the Firepower Management Center (FMC) Software.

An XSS flaw in GitLab allows attackers to take over accounts

Security Affairs - 24 May 2024 21:39

GitLab addressed a high-severity cross-site scripting (XSS) vulnerability that allows unauthenticated attackers to take over user accounts. GitLab fixed a high-severity XSS vulnerability, tracked as CVE-2024-4835, that allows attackers to take over user accounts. An attacker can exploit this issue by using a specially crafted page to exfiltrate sensitive user information.

WordPress Plugin Exploited to Steal Credit Card Data from E-commerce Sites

The Hacker News - 28 May 2024 13:00

Unknown threat actors are abusing lesser-known code snippet plugins for WordPress to insert malicious PHP code in victim sites that are capable of harvesting credit card data.The campaign, observed by Sucuri on May 11, 2024, entails the abuse of a WordPress plugin called Dessky Snippets, which allows users to add custom PHP code. It has over 200 active installations.

Experts Find Flaw in Replicate AI Service Exposing Customers' Models and Data

The Hacker News - 25 May 2024 15:41

Cybersecurity researchers have discovered a critical security flaw in an artificial intelligence (AI)-as-a-service provider Replicate that could have allowed threat actors to gain access to proprietary AI models and sensitive information. "Exploitation of this vulnerability would have allowed unauthorized access to the AI prompts and results of all Replicate's platform customers."

Scottish Cyber Coordination Centre

Update Chrome Browser Now: 4th Zero-Day Exploit Discovered in May 2024

The Hacker News - 24 May 2024 16:40

Google on Thursday rolled out fixes to address a high-severity security flaw in its Chrome browser that it said has been exploited in the wild.Assigned the CVE identifier CVE-2024-5274, the vulnerability relates to a type confusion bug in the V8 JavaScript and WebAssembly engine.

Threat actors and malware

Hackers phish finance orgs using trojanized Minesweeper clone

BleepingComputer - 26 May 2024 11:16

Hackers are utilizing code from a Python clone of Microsoft's venerable Minesweeper game to hide malicious scripts in attacks on European and US financial organizations. [...]

Arc browser's Windows launch targeted by Google ads malvertising

BleepingComputer - 25 May 2024 12:17

A new Google Ads malvertising campaign, coinciding with the launch of the Arc web browser for Windows, was tricking people into downloading trojanized installers that infect them with malware payloads. [...]

New ShrinkLocker ransomware uses BitLocker to encrypt your files

BleepingComputer - 24 May 2024 11:59

A new ransomware strain called ShrinkLocker creates a new boot partition to encrypt corporate systems using Windows BitLocker. [...]

New ATM Malware family emerged in the threat landscape

Security Affairs - 27 May 2024 12:20

Experts warn of a new ATM malware family that is advertised in the cybercrime underground, it was developed to target Europe. A threat actor is advertising a new ATM malware family that claims to be able of compromised 99% of devices in Europe. The threat actor is offering the malware for $30,000, he claims that [...]

CERT-UA warns of malware campaign conducted by threat actor UAC-0006

Security Affairs - 26 May 2024 17:45

The Ukraine CERT-UA warns of a concerning increase in cyberattacks attributed to the financially-motivated threat actor UAC-0006. The Computer Emergency Response Team of Ukraine (CERT-UA) warned of surge in in cyberattacks linked to the financially-motivated threat actor UAC-0006.

Malware-laced JAVS Viewer deploys RustDoor implant in supply chain attack

Security Affairs - 26 May 2024 05:11

Scottish Cyber Coordination Centre

Malicious actors compromised the JAVS Viewer installer to deliver the RustDoor malware in a supply chain attack. Rapid7 researchers warned that threat actors added a backdoor to the installer for the Justice AV Solutions JAVS Viewer software.

Stealthy BLOODALCHEMY Malware Targeting ASEAN Government Networks

The Hacker News - 24 May 2024 15:43

Cybersecurity researchers have discovered that the malware known as BLOODALCHEMY used in attacks targeting government organizations in Southern and Southeastern Asia is in fact an updated version of Deed RAT, which is believed to be a successor to ShadowPad.