Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 August 2024

Vulnerabilities

Google fixes ninth Chrome zero-day exploited in attacks this year

BleepingComputer - 21 August 2024 18:43

Today, Google released a new Chrome emergency security update to patch a zero-day vulnerability, the ninth one exploited in attacks this year.

GitHub Enterprise Server vulnerable to critical auth bypass flaw

BleepingComputer - 21 August 2024 11:15

A critical vulnerability affecting multiple versions of GitHub Enterprise Server could be exploited to bypass authentication and enable an attacker to gain administrator privileges on the machine.

Experts disclosed a critical information-disclosure flaw in Microsoft Copilot Studio

Security Affairs - 21 August 2024 20:36

Researchers have disclosed a critical security vulnerability in Microsoft's Copilot Studio that could lead to the exposure of sensitive information. Researchers disclosed a critical security vulnerability, tracked as CVE-2024-38206 (CVSS score: 8.5), impacting Microsoft's Copilot Studio.

Critical Flaw in WordPress LiteSpeed Cache Plugin Allows Hackers Admin Access

The Hacker News - 22 August 2024 11:32

Cybersecurity researchers have disclosed a critical security flaw in the LiteSpeed Cache plugin for WordPress that could permit unauthenticated users to gain administrator privileges. The plugin suffers from an unauthenticated privilege escalation vulnerability which allows any unauthenticated visitor to gain Administrator level access.

Exploits and vulnerabilities in Q2 2024

Securelist - 21 August 2024 11:00

The report contains statistics on vulnerabilities and exploits, with an analysis of interesting vulnerabilities found in Q2 2024.

Scottish Cyber Coordination Centre

Threat actors and malware

North Korea-linked APT used a new RAT called MoonPeak

Security Affairs - 21 August 2024 18:26

North Korea-linked APT Kimsuky is likely behind a new remote access trojan called MoonPeak used in a recent campaign spotted by Cisco Talos. Cisco Talos researchers uncovered the infrastructure used by the North Korea-linked APT group tracked as UAT-5394, which experts suspect is linked to the Kimsuky APT group.

New macOS Malware TodoSwift Linked to North Korean Hacking Groups

The Hacker News - 21 August 2024 17:30

Cybersecurity researchers have uncovered a new macOS malware strain dubbed TodoSwift that they say exhibits commonalities with known malicious software used by North Korean hacking groups.

110K domains targeted in 'sophisticated' AWS cloud extortion campaign

The Register - 21 August 2024 18:23

Security shop Cyble released some research this week after finding 110,000 domains targeted by attackers exploiting misconfigured .env files, which typically contain secrets such as hard-coded cloud access keys.

Thousands of Apps Using AWS ALB Exposed to Attacks Due to Configuration Issue

SecurityWeek - 21 August 2024 13:40

As many as 15,000 applications using AWS Application Load Balancer (ALB) could be exposed to ALBeast attacks.

ASD's ACSC, CISA, FBI, and NSA, with the support of International Partners Release Best Practices for Event Logging and Threat Detection

CISA Advisories -

Today, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), CISA, FBI, NSA, and international partners are releasing Best Practices for Event Logging and Threat Detection. This guide will assist organizations in defining a baseline for event logging to mitigate malicious cyber threats.