Scottish Cyber Coordination Centre

Daily threat bulletin

10 June 2024

Vulnerabilities

PHP fixes critical RCE flaw impacting all versions for Windows

BleepingComputer - 07 June 2024 11:32

A new PHP for Windows remote code execution (RCE) vulnerability has been disclosed, impacting all releases since version 5.x, potentially impacting a massive number of servers worldwide.

SolarWinds fixed multiple flaws in Serv-U and SolarWinds Platform

Security Affairs - 07 June 2024 22:37

SolarWinds addressed multiple vulnerabilities in Serv-U and the SolarWinds Platform, including a bug reported by a pentester working with NATO. SolarWinds announced security patches to address multiple high-severity vulnerabilities in Serv-U and the SolarWinds Platform.

Chinese threat actor exploits old ThinkPHP flaws since October 2023

Security Affairs - 07 June 2024 08:38

Akamai researchers observed a Chinese threat actor exploiting two old remote code execution vulnerabilities, tracked as CVE-2018-20062 and CVE-2019-9082, in ThinkPHP. The campaign seems to have been active since at least October 2023.

Cisco fixes WebEx flaw that allowed government, military meetings to be spied on

The Register - 07 June 2024 16:04

Researchers were able to glean data from 10,000 meetings held by top Dutch gov officials. Cisco squashed some bugs this week that allowed anyone to view WebEx meeting information and join them, potentially opening up security and privacy concerns for highly sensitive meetings.

EmailGPT Exposed to Prompt Injection Attacks

Infosecurity Magazine - 07 June 2024 14:00

The flaw enables attackers to gain control over the AI service by submitting harmful prompts.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2017-3506 Oracle WebLogic Server OS Command Injection Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

DDoS attacks target EU political parties as elections begin

BleepingComputer - 08 June 2024 11:12

Hacktivists are conducting DDoS attacks on European political parties that represent and promote strategies opposing their interests, according to a report by Cloudflare.

FBI Distributes 7,000 LockBit Ransomware Decryption Keys to Help Victims

The Hacker News - 07 June 2024 14:18

The U.S. Federal Bureau of Investigation (FBI) has disclosed that it's in possession of more than 7,000 decryption keys associated with the LockBit ransomware operation to help victims get their data back at no cost.

SPECTR Malware Targets Ukraine Defense Forces in SickSync Campaign

The Hacker News - 07 June 2024 13:43

The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of cyber attacks targeting defense forces in the country with a malware called SPECTR as part of an espionage campaign dubbed SickSync.The agency attributed the attacks to a threat actor it tracks under the moniker UAC-0020, which is also called Vermin.

Commando Cat Cryptojacking Attacks Target Misconfigured Docker Instances

The Hacker News - 07 June 2024 11:40

The threat actor known as Commando Cat has been linked to an ongoing cryptojacking attack campaign that leverages poorly secured Docker instances to deploy cryptocurrency miners for financial gain.