Scottish
Cyber
Coordination
Centre

Daily threat bulletin

3 June 2024

Vulnerabilities

Critical Apache Log4j2 flaw still threatens global finance

Security Affairs - 01 June 2024 16:44

The vulnerability CVE-2021-44832 in Apache Log4j2 library is still a serious problem for multiple industries, expert warns it threatens global Finance. The independent cyber threat intelligence analyst Anis Haboubi warns of a severe logging configuration flaw that could dramatically impact the financial industry.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-24919 Check Point Quantum Security Gateways Information Disclosure Vulnerability; CVE-2024-1086 Linux Kernel Use-After-Free Vulnerability.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-4978 Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2024-5274 Google Chromium V8 Type Confusion Vulnerability.

Threat actors and malware

Snowflake account hacks linked to Santander, Ticketmaster breaches

BleepingComputer - 31 May 2024 14:31

A threat actor claiming recent Santander and Ticketmaster breaches says they stole data after hacking into an employee’s account at cloud storage company Snowflake. However, Snowflake disputes these claims, saying recent breaches were caused by poorly secured customer accounts. [...]

Over 600,000 SOHO routers were destroyed by Chalubo malware in 72 hours

Security Affairs - 31 May 2024 14:34

The Chalubo trojan destroyed over 600,000 SOHO routers from a single ISP, researchers from Lumen Technologies reported. Between October 25 and October 27, 2023, the Chalubo malware destroyed more than 600,000 small office/home office (SOHO) routers belonging to the same ISP.

LilacSquid APT targeted organizations in the U.S., Europe, and Asia since at least 2021

Security Affairs - 31 May 2024 12:19

A previously undocumented APT group tracked as LilacSquid targeted organizations in the U.S., Europe, and Asia since at least 2021. Cisco Talos researchers reported that a previously undocumented APT group, tracked as LilacSquid, conducted a data theft campaign since at least 2021.

Beware: Fake Browser Updates Deliver BitRAT and Lumma Stealer Malware

The Hacker News - 03 June 2024 10:21

Fake web browser updates are being used to deliver remote access trojans (RATs) and information stealer malware such as BitRAT and Lumma Stealer (aka LummaC2)."Fake browser updates have been responsible for numerous malware infections, including those of the well-known SocGholish malware," cybersecurity firm eSentire said in a new report.

Russian Hackers Target Europe with HeadLace Malware and Credential Harvesting

The Hacker News - 31 May 2024 16:40

The Russian GRU-backed threat actor APT28 has been attributed as behind a series of campaigns targeting networks across Europe with the HeadLace malware and credential-harvesting web pages.

OpenAI, Meta, and TikTok Crack Down on Covert Influence Campaigns, Some AI-Powered

The Hacker News - 31 May 2024 14:41

OpenAI on Thursday disclosed that it took steps to cut off five covert influence operations (IO) originating from China, Iran, Israel, and Russia that sought to abuse its artificial intelligence (AI) tools to manipulate public discourse or political outcomes online while obscuring their true identity.

FlyingYeti APT Serves Up Cookbox Malware Using WinRAR

darkreading - 31 May 2024 16:10

The Russia-aligned FlyingYeti's phishing campaign exploited Ukrainian citizens' financial stress to spread Cookbox malware.