Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 June 2025

Vulnerabilities

New Veeam RCE flaw lets domain users hack backup servers

BleepingComputer - 17 June 2025 12:42

Veeam has released security updates today to fix several Veeam Backup & Replication (VBR) flaws, including a critical remote code execution (RCE) vulnerability. [...]

Sitecore CMS exploit chain starts with hardcoded 'b' password

BleepingComputer - 17 June 2025 12:10

A chain of Sitecore Experience Platform (XP) vulnerabilities allows attackers to perform remote code execution (RCE) without authentication to breach and hijack servers. [...]

U.S. CISA adds Apple products, and TP-Link routers flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 17 June 2025 14:15

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Apple products, and TP-Link routers flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Apple products, and TP-Link routers flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Attackers target Zyxel RCE vulnerability CVE-2023-28771

Security Affairs - 17 June 2025 11:34

GreyNoise researchers have observed exploit attempts targeting the remote code execution vulnerability CVE-2023-28771 in Zyxel devices. On June 16, GreyNoise researchers detected exploit attempts targeting CVE-2023-28771 (CVSS score 9.8), a remote code execution flaw impacting Zyxel IKE decoders over UDP port 500. "Exploitation attempts against CVE-2023-28771 were minimal throughout recent weeks.

Google Chrome Zero-Day CVE-2025-2783 Exploited by TaxOff to Deploy Trinper Backdoor

The Hacker News - 18 June 2025 01:46

A now-patched security flaw in Google Chrome was exploited as a zero-day by a threat actor known as TaxOff to deploy a backdoor codenamed Trinper.The attack, observed in mid-March 2025 by Positive Technologies, involved the use of a sandbox escape vulnerability tracked as CVE-2025-2783 (CVSS score: 8.3).Google addressed the flaw later that month after Kaspersky reported in-the-wild

Scottish Cyber Coordination Centre

LangSmith Bug Could Expose OpenAI Keys and User Data via Malicious Agents

The Hacker News - 18 June 2025 00:03

Cybersecurity researchers have disclosed a now-patched security flaw in LangChain's LangSmith platform that could be exploited to capture sensitive data, including API keys and user prompts.The vulnerability, which carries a CVSS score of 8.8 out of a maximum of 10.0, has been codenamed AgentSmith by Noma Security.

New Flodrix Botnet Variant Exploits Langflow AI Server RCE Bug to Launch DDoS Attacks

The Hacker News - 17 June 2025 16:02

Cybersecurity researchers have called attention to a new campaign that's actively exploiting a recently disclosed critical security flaw in Langflow to deliver the Flodrix botnet malware.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2023-0386 Linux Kernel Improper Ownership Management 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

Iran Slows Internet to Prevent Cyber Attacks Amid Escalating Regional Conflict

The Hacker News - 18 June 2025 12:05

Iran has throttled internet access in the country in a purported attempt to hamper Israel's ability to conduct covert cyber operations, days after the latter launched an unprecedented attack on the country, escalating geopolitical tensions in the region.

Silver Fox APT Targets Taiwan with Complex Gh0stCringe and HoldingHands RAT Malware

The Hacker News - 17 June 2025 19:58

Cybersecurity researchers are warning of a new phishing campaign that's targeting users in Taiwan with malware families such as HoldingHands RAT and Gh0stCringe.

Google Warns of Scattered Spider Attacks Targeting IT Support Teams at U.S. Insurance Firms

The Hacker News - 17 June 2025 19:23

The notorious cybercrime group known as Scattered Spider (aka UNC3944) that recently targeted various U.K. and U.S. retailers has begun to target major insurance companies, according to Google Threat Intelligence Group (GTIG).

New ClickFix Malware Variant 'LightPerlGirl' Targets Users in Stealthy Hack

Scottish Cyber Coordination Centre

SecurityWeek - 17 June 2025 21:36

Researchers identify a previously unknown ClickFix variant exploiting PowerShell and clipboard hijacking to deliver the Lumma infostealer via a compromised travel site.

UK related

UK fines 23andMe for 'profoundly damaging' breach exposing genetics data

BleepingComputer - 17 June 2025 11:59

The UK Information Commissioner's Office (ICO) has fined genetic testing provider 23andMe £2.31 million ($3.12 million) over 'serious security failings' that led to a 'profoundly damaging' data breach in 2023.