Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 May 2025

Vulnerabilities

ViciousTrap Uses Cisco Flaw to Build Global Honeypot from 5,300 Compromised Devices

The Hacker News - 23 May 2025 19:19

Cybersecurity researchers have disclosed that a threat actor codenamed ViciousTrap has compromised nearly 5,300 unique network edge devices across 84 countries and turned them into a honeypot-like network.

CISA Warns of Suspected Broader SaaS Attacks Exploiting App Secrets and Cloud Misconfigs

The Hacker News - 23 May 2025 11:46

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday revealed that Commvault is monitoring cyber threat activity targeting applications hosted in their Microsoft Azure cloud environment.

GitLab Duo Vulnerability Enabled Attackers to Hijack AI Responses with Hidden Prompts

The Hacker News - 23 May 2025 11:04

Cybersecurity researchers have discovered an indirect prompt injection flaw in GitLab's artificial intelligence (AI) assistant Duo that could have allowed attackers to steal source code and inject untrusted HTML into its responses, which could then be used to direct victims to malicious websites.

Companies Warned of Commvault Vulnerability Exploitation

SecurityWeek - 23 May 2025 11:31

CISA warns companies of a widespread campaign targeting a Commvault vulnerability to hack Azure environments.

NIST Introduces New Metric to Measure Likelihood of Vulnerability Exploits

Infosecurity Magazine - 26 May 2025 10:00

The US National Institute of Standards and Technology (NIST) published a white paper introducing a new metric called Likely Exploited Vulnerabilities (LEV)

Threat actors and malware

Fake Zenmap. WinMRT sites target IT staff with Bumblebee malware

BleepingComputer - 24 May 2025 11:26

The Bumblebee malware SEO poisoning campaign uncovered earlier this week aimpersonating RVTools is using more typosquatting domainsi mimicking other popular open-source projects to infect devices used by IT staff. [...]

China-linked APT UNC5221 started exploiting Ivanti EPMM flaws shortly after their disclosure

Security Affairs - 26 May 2025 12:31

China-linked APT exploit Ivanti EPMM flaws to target critical sectors across Europe, North America, and Asia-Pacific, according to EclecticIQ. Researchers from EclecticIQ observed a China-linked APT group that chained two Ivanti EPMM flaws, tracked as CVE-2025-4427 and CVE-2025-4428, in attacks against organizations in Europe, North America, and Asia-Pacific.

Operation ENDGAME disrupted global ransomware infrastructure

Security Affairs - 25 May 2025 10:39

Operation ENDGAME dismantled key ransomware infrastructure, taking down 300 servers, 650 domains, and seizing €21.2M in crypto. From May 19 to 22, 2025, Operation ENDGAME, coordinated by Europol and Eurojust, disrupted global ransomware infrastructure.

Chinese threat actors exploited Trimble Cityworks flaw to breach U.S. local government networks

Security Affairs - 23 May 2025 07:27

A Chinese threat actor, tracked as UAT-6382, exploited a patched Trimble Cityworks flaw to deploy Cobalt Strike and VShell.

Hackers Use Fake VPN and Browser NSIS Installers to Deliver Winos 4.0 Malware

The Hacker News - 25 May 2025 14:06

Cybersecurity researchers have disclosed a malware campaign that uses fake software installers masquerading as popular tools like LetsVPN and QQ Browser to deliver the Winos 4.0 framework.