Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 September 2025

Vulnerabilities

CISA Warns of Two Malware Strains Exploiting Ivanti EPMM CVE-2025-4427 and CVE-2025-4428

The Hacker News - 19 September 2025 10:40

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday released details of two sets of malware that were discovered in an unnamed organization's network following the exploitation of security flaws in Ivanti Endpoint Manager Mobile (EPMM).

Microsoft Entra ID flaw allowed hijacking any company's tenant

BleepingComputer - 21 September 2025 14:30

A critical combination of legacy components could have allowed complete access to the Microsoft Entra ID tenant of every company in the world. [...]

Fortra addressed a maximum severity flaw in GoAnywhere MFT software

Security Affairs - 19 September 2025 18:32

Fortra addressed a critical flaw in GoAnywhere Managed File Transfer (MFT) software that could result in the execution of arbitrary commands. Fortra addressed a critical vulnerability, tracked as CVE-2025-10035 (CVSS score of 10.0) in GoAnywhere Managed File Transfer (MFT) software.

ShadowLeak Zero-Click Flaw Leaks Gmail Data via OpenAI ChatGPT Deep Research Agent

The Hacker News - 20 September 2025 12:01

Cybersecurity researchers have disclosed a zero-click flaw in OpenAI ChatGPT's Deep Research agent that could allow an attacker to leak sensitive Gmail inbox data with a single crafted email without any user action.

Fortra Releases Critical Patch for CVSS 10.0 GoAnywhere MFT Vulnerability

The Hacker News - 19 September 2025 20:42

Fortra has disclosed details of a critical security flaw in GoAnywhere Managed File Transfer (MFT) software that could result in the execution of arbitrary commands.

Threat actors and malware

CISA exposes malware kits deployed in Ivanti EPMM attacks

BleepingComputer - 19 September 2025 12:46

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has published an analysis of the malware deployed in attacks exploiting vulnerabilities affecting Ivanti Endpoint Manager Mobile (EPMM). [...]

A cyberattack on Collins Aerospace disrupted operations at major European airports

Security Affairs - 20 September 2025 17:43

A cyberattack on Collins Aerospace disrupted operations at major European airports, with Heathrow, Brussels, and Berlin most affected. A cyber attack on Collins Aerospace disrupted check-in and boarding systems at major European airports, heavily impacting Heathrow, Brussels, and Berlin.

Researchers Uncover GPT-4-Powered MalTerminal Malware Creating Ransomware, Reverse Shell

The Hacker News - 20 September 2025 12:18

Cybersecurity researchers have discovered what they say is the earliest example known to date of a malware that bakes in Large Language Model (LLM) capabilities.

17,500 Phishing Domains Target 316 Brands Across 74 Countries in Global PhaaS Surge

The Hacker News - 19 September 2025 20:32

The phishing-as-a-service (PhaaS) offerings known as Lighthouse and Lucid has been linked to more than 17,500 phishing domains targeting 316 brands from 74 countries.

UK related

UK police arrested two teen Scattered Spider members linked to the 2024 attack on Transport for London

Security Affairs - 19 September 2025 11:54

U.K. police arrested two teens from the Scattered Spider group for their role in the August 2024 cyberattack on Transport for London. U.K. law enforcement authorities arrested two teenagers who are members of the notorious Scattered Spider hacking group in connection with their role in the cyber attack that hit Transport for London (TfL).

Heathrow warns of second day of disruption after cyber-attack

BBC News - 21 September 2025 17:29

The issue affecting check-in and baggage systems caused hundreds of delays and cancellations on Saturday.