Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 August 2025

Vulnerabilities

Over 28,000 Citrix devices vulnerable to new exploited RCE flaw

BleepingComputer - 27 August 2025 13:48

More than 28,200 Citrix instances are vulnerable to a critical remote code execution vulnerability tracked as CVE-2025-7775 that is already being exploited in the wild. [...]

U.S. CISA adds Citrix NetScaler flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 27 August 2025 19:20

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Citrix NetScaler flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Citrix NetScaler flaw, tracked as CVE-2025-7775, to its Known Exploited Vulnerabilities (KEV) catalog.

Threat actors and malware

Storm-0501 hackers shift to ransomware attacks in the cloud

BleepingComputer - 27 August 2025 19:38

Microsoft warns that a threat actor tracked as Storm-0501 has evolved its operations, shifting away from encrypting devices with ransomware to focusing on cloud-based encryption, data theft, and extortion. [...]

Someone Created the First AI-Powered Ransomware Using OpenAI's gpt-oss:20b Model

The Hacker News - 27 August 2025 23:37

Cybersecurity company ESET has disclosed that it discovered an artificial intelligence (AI)-powered ransomware variant codenamed PromptLock.Written in Golang, the newly identified strain uses the gpt-oss:20b model from OpenAI locally via the Ollama API to generate malicious Lua scripts in real-time. The open-weight language model was released by OpenAI earlier this month.

Anthropic Disrupts AI-Powered Cyberattacks Automating Theft and Extortion Across Critical Sectors

The Hacker News - 27 August 2025 21:40

Anthropic on Wednesday revealed that it disrupted a sophisticated operation that weaponized its artificial intelligence (AI)-powered chatbot Claude to conduct large-scale theft and extortion of personal data in July 2025."The actor targeted at least 17 distinct

organizations, including in healthcare, the emergency services, and government, and religious institutions," the company said. "

NSA, FBI, Others Say Chinese Tech Firms are Aiding Salt Typhoon Attacks

Security Boulevard - 28 August 2025 06:08

A report from intelligence agencies in the U.S., UK, and elsewhere outlined how three Chinese tech firms are supply China's intelligence services with products and services that are being used in global campaigns by the state-sponsored APT group Salt Typhoon.