Scottish Cyber Coordination Centre

Daily threat bulletin

5 November 2024

Vulnerabilities

Critical Flaws in Ollama AI Framework Could Enable DoS, Model Theft, and Poisoning

The Hacker News - 04 November 2024 20:38

Cybersecurity researchers have disclosed six security flaws in the Ollama artificial intelligence (AI) framework that could be exploited by a malicious actor to perform various actions, including denial-of-service, model poisoning, and model theft.

Okta Fixes Auth Bypass Bug After 3-Month Lull

darkreading - 04 November 2024 21:54

The bug affected accounts with 52-character user names, and had several pre-conditions that needed to be met in order to be exploited.

Google: Big Sleep AI Agent Puts SQLite Software Bug to Bed

darkreading - 04 November 2024 16:46

A research tool by the company found a vulnerability in the SQLite open source database, demonstrating the "defensive potential" for using LLMs to find vulnerabilities in applications before they're publicly released.

Hackers Exploit DocuSign APIs for Phishing Campaign

Security Boulevard - 05 November 2024 08:18

Cybercriminals are exploiting DocuSign's APIs to send highly authentic-looking fake invoices, while DocuSign's forums have reported a rise in such fraudulent campaigns in recent months. Unlike typical phishing scams that rely on spoofed emails and malicious links, these attacks use legitimate DocuSign accounts and templates to mimic reputable companies, according to a Wallarm report. By.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2024-8957 PTZOptics PT30X-SDI/NDI Cameras OS Command Injection VulnerabilityCVE-2024-8956 PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability.

Fortinet Updates Guidance and Indicators of Compromise following FortiManager Vulnerability Exploitation

CISA Advisories -

Fortinet has updated their security advisory addressing a critical FortiManager vulnerability (CVE-2024-47575) to include additional workarounds and indicators of compromise (IOCs). A remote, unauthenticated cyber threat actor could exploit this vulnerability to gain access to sensitive files or take control of an affected system.

Threat actors and malware

Nokia investigates breach after hacker claims to steal source code

BleepingComputer - 04 November 2024 19:47

Nokia is investigating whether a third-party vendor was breached after a hacker claimed to be selling the company's stolen source code. [...]

Custom "Pygmy Goat" malware used in Sophos Firewall hack on govt network

BleepingComputer - 04 November 2024 13:46

UK's National Cyber Security Centre (NCSC) has published an analysis of a Linux malware named "Pigmy Goat" created to backdoor Sophos XG firewall devices as part of recently disclosed attacks by Chinese threat actors. [...]

Windows infected with backdoored Linux VMs in new phishing attacks

BleepingComputer - 04 November 2024 11:53

A new phishing campaign dubbed 'CRON#TRAP' infects Windows with a Linux virtual machine that contains a built-in backdoor to give stealthy access to corporate networks. [...]

Schneider Electric says hackers accessed internal project execution tracking platform

The Record from Recorded Future News - 05 November 2024 02:05

Cisco notifies 'limited set' of customers after hacker accessed non-public files

The Record from Recorded Future News - 04 November 2024 21:56