Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 August 2026

Vulnerabilities

U.S. CISA adds Langflow, Apache Tomcat, and N-able N-central flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 05 August 2026 16:25

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Langflow, Apache Tomcat, and N-able N-central flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog:

Paperclip AI Flaws Let Attackers Run Host Commands via Malicious Agent Imports

The Hacker News - 05 August 2026 21:44

Two security flaws in Paperclip could let attackers execute commands on a network server or a developer's computer.

Veeam, Terraform MCP, Django Patch Critical Flaws, Led by CVSS 10.0 Cross-Tenant Bug

The Hacker News - 05 August 2026 20:57

HashiCorp, Veeam, and the Django Software Foundation have patched 11 vulnerabilities across Terraform MCP Server, Veeam Service Provider Console, and Django.

New OVSwrap Linux Kernel Flaw Lets Local Users Gain Root via Open vSwitch

The Hacker News - 05 August 2026 18:13

A memory corruption flaw in the Linux kernel's Open vSwitch datapath gives ordinary local users a path to root on a broad set of default-configured distributions, and a public exploit ships with pre-built records for roughly 800 kernel builds.

Critical Gitea Flaw Let Unauthenticated Attackers Read Server Files via Org-Mode Markup

The Hacker News - 05 August 2026 17:34

An unauthenticated attacker can read any file the service account can access on Gitea, the self-hosted Git platform, in versions 1.22.1 through 1.27.0.

Cisco Patches Critical SD-WAN, IOS XE, FMC Vulnerabilities

SecurityWeek - 06 August 2026 08:20

Patches were rolled out for two dozen vulnerabilities, including one with public proof-of-concept (PoC) code.

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers run khunt post-exploitation toolkit from Oracle database

BleepingComputer - 05 August 2026 16:55

Hackers exploited a SQL injection vulnerability to install a post-exploitation toolkit directly inside an Oracle database that was used to breach a corporate network. [...]

Trojanized npm Packages Employ NullReceiver Tactic to Decode C2 IP from Blockchain

The Hacker News - 05 August 2026 20:11

Cybersecurity researchers have flagged an evolution of the EtherHiding blockchain-based command-and-control (C2) technique that conceals the C2 server IP address inside a made-up destination address of a completely empty Ethereum transfer.

QuickFox Supply Chain Attack Delivers FDMTP Backdoor via Trojanized Windows Installer

The Hacker News - 05 August 2026 12:17

Cybersecurity researchers have disclosed what has been described as a “long-standing supply chain attack” on QuickFox, a virtual private network (VPN) and network acceleration tool designed for overseas Chinese users.

Flaws in Google APK for Python Unlock Agent-to-Agent Attack

darkreading - 05 August 2026 19:03

Google has fixed the issues, which exploited a trust boundary between two AI agents with different privilege levels to trigger automation that could compromise the supply chain.

Chinese router vendor denies its firmware contains backdoors – but pauses downloads to fix security issues anyway

The Register - 06 August 2026 07:57

It’s just a remote maintenance function, says Zbtlink

OpenAI reveals its rogue agent swarm went a little bit Borg ahead of Hugging Face hack

The Register - 06 August 2026 04:47

It started with an ‘impossible task’ and led to AI deciding it needed to act as a collective intelligence

UK related

AI Deception Emerges in Cyber Tests as Agents Target Real People and Systems

Scottish Cyber Coordination Centre

Security Affairs - 05 August 2026 20:39

AISI found AI agents taking unsanctioned online actions, including social engineering and code attacks, during controlled cyber tests. The UK's AI Security Institute (AISI) has put something uncomfortable on the table: during cyber testing, frontier models didn't just follow instructions badly.

UK charities count the cost of Beacon CRM cyberattack

The Register - 05 August 2026 14:04

Database backups likely stolen, potentially exposing donor, supporter, and service user details