Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 July 2026

Vulnerabilities

New Januscape Linux flaw allows VM escape on Intel, AMD devices

BleepingComputer - 07 July 2026 09:06

A 16-year-old Linux kernel vulnerability, dubbed Januscape, allows attackers to escape a virtual machine and execute arbitrary code on the host.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2026-48908 JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability
CVE-2026-55255 Langflow Authorization Bypass Through User-Controlled Key Vulnerability
CVE-2026-56290 Joomlack Page Builder Improper Access Control Vulnerability

Critical Adobe ColdFusion Vulnerability Exploited in Attacks

SecurityWeek - 07 July 2026 13:38

Hackers are exploiting a recently patched critical vulnerability (CVE-2026-48282) in Adobe ColdFusion that carries a CVSS score of 10/10.

Critical Gitea Docker Bug Under Active Exploitation Exposes Repositories and Secrets

Security Affairs - 07 July 2026 22:16

Sysdig researchers warn that attackers are actively exploiting a critical authentication bypass flaw, tracked as CVE-2026-20896 (CVSS score of 9.8), which affects Gitea official Docker images before version 1.26.3.

BeyondTrust Patches Critical Auth Bypass Flaws in Remote Support and PRA

The Hacker News - 07 July 2026 11:46

BeyondTrust has released updates to address two critical security flaws affecting Remote Support (RS) and Privileged Remote Access (PRA) products that, if successfully exploited, could allow unauthenticated attackers to take control of susceptible devices.

Scottish Cyber Coordination Centre

Threat actors and malware

Chinese hackers develop LONGLEASH malware to expand ORB network

BleepingComputer - 07 July 2026 15:52

Chinese hackers tracked as 'UAT-7810' are actively evolving their malware to expand their Operational Relay Box (ORB) network by compromising internet-facing networking devices, primarily unpatched Ruckus routers.

Accenture confirms breach after hacker offers stolen data for sale

BleepingComputer - 07 July 2026 19:06

IT services giant Accenture has confirmed it suffered a security breach after a threat actor claimed to have stolen 35 GB of source code and other data from the company.

AI-Generated Malware Powers New Armored Likho APT Campaign

Security Affairs - 07 July 2026 09:28

Armored Likho APT uses AI-generated malware, phishing, and BusySnake Stealer to target governments and power grids in Russia, Kazakhstan, and Brazil. Kaspersky's threat research team has documented a previously unknown APT group they're calling Armored Likho, also tracked under the name Eagle Werewolf.

DEBULL Tooling Abuses Microsoft Device-Code Flow to Target M365 Accounts

The Hacker News - 07 July 2026 21:44

A Microsoft 365 device code phishing campaign has been observed leveraging collaboration-themed lures to take control of victim accounts between the last week of June 2026 and into early July, per findings from ZeroBEC.

Iran-Linked Hackers Using Modular C&C Framework in Cyberattacks

SecurityWeek - 07 July 2026 13:21

Researchers say the Iran-linked threat actor used an adaptable modular malware framework and compromised IT service providers to reach high-value targets in Israel.

UK incidents

UK Government Launches Cyber Resilience Pledge, Claiming 60+ Signatories

Infosecurity Magazine - 07 July 2026 11:00

More than 60 organizations, including M&S, Microsoft UK and Vodafone, have signed the UK government's Cyber Resilience Pledge, a new initiative aimed at boosting cyber security and resilience across British businesses.