Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 July 2026

Vulnerabilities

Max severity Adobe ColdFusion flaw now exploited in attacks

BleepingComputer - 06 July 2026 10:18

Attackers are now exploiting a maximum-severity Adobe ColdFusion vulnerability tracked as CVE-2026-48282, according to vulnerability intelligence company KEVIntel. [...]

Bad Epoll Flaw Gives Attackers Root Access on Linux and Android

Security Affairs - 06 July 2026 09:24

Bad Epoll (CVE-2026-46242) lets local attackers gain root on Linux and Android. The flaw was missed by AI but found by a security researcher. A newly disclosed Linux kernel vulnerability, named Bad Epoll (CVE-2026-46242), allows a local attacker with no special privileges to gain full root access on affected Linux systems and Android devices.

Threat Actors Probe Gitea Docker Flaw CVE-2026-20896 13 Days After Disclosure

The Hacker News - 06 July 2026 22:58

Threat actors have been observed attempting to exploit a recently patched critical security flaw in Gitea Docker images, according to Sysdig.The vulnerability in question is CVE-2026-20896 (CVSS score: 9.8), a vulnerability that stems from the DevOps platform trusting the “X-WEBAUTH-USER” header from any source IP address, effectively allowing an unauthenticated internet client to get elevated

Opera GX Flaw Let Malicious Sites Auto-Install Mods to Steal Data From Visited Pages

The Hacker News - 06 July 2026 13:57

Researchers found a flaw in Opera GX, the gaming-focused version of the Opera browser, that let a malicious website silently install a browser add-on and use it to lift specific data from the pages a victim visits.In a proof of concept, they reconstructed a signed-in user’s full Gmail address from a single visit, with no click.

Threat actors and malware

Fake IT support calls on Microsoft Teams push EtherRAT malware

BleepingComputer - 06 July 2026 17:23

Threat actors are abusing Microsoft Teams voice calls by impersonating corporate IT support staff to trick employees into installing the EtherRAT malware, giving attackers initial access to corporate networks. [...]

Scottish Cyber Coordination Centre

Suspected China-Nexus Hackers Use Fake Indian Tax Filing Utility to Deploy DcRAT

The Hacker News - 06 July 2026 17:28

A suspected China-nexus threat activity cluster has been observed targeting Indian taxpayers, tax professionals, and corporate finance teams to deliver a remote access trojan designed to steal sensitive data from compromised hosts.

New TrojPix Attack Leaks Data From Air-Gapped Systems via Video Cable Emissions

The Hacker News - 06 July 2026 15:20

Researchers at Shandong University have shown a fast new way to pull data off computers that are cut off from every network. The technique, called TrojPix, tweaks on-screen pixels in ways the eye cannot see, so that the video cable carrying them radiates a faint radio signal a nearby receiver can decode.

Researchers Discover First Documented Case of Agentic Ransomware

Security Magazine - 06 July 2026 12:00

Researchers believe they have discovered the first documented case of an extortion operation run end-to-end by an LLM.

Armored Likho APT Targeting Government, Electric Power Entities

SecurityWeek - 06 July 2026 16:10

The threat actor uses modular RATs and information stealers in financially motivated and cyber espionage campaigns.

New Iran-Nexus Hacking Group Targets Israel Government and IT Sectors

Infosecurity Magazine - 06 July 2026 17:00

Check Point researchers have identified a new cyber adversary targeting Israeli government and IT businesses, tracked as ‘Cavern Manticore’