Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 July 2026

Vulnerabilities

Microsoft patches RoguePlanet Defender zero-day vulnerability

BleepingComputer - 09 July 2026 02:42

Microsoft has released a security patch to address a Defender zero-day vulnerability known as “RoguePlanet,” disclosed after the June 2026 Patch Tuesday.

Google Dialogflow CX Bug Allowed Attackers to Hijack AI Conversations

SecurityWeek - 08 July 2026 13:15

The “Rogue Agent” vulnerability could have enabled attackers to silently manipulate AI conversations, exfiltrate data, and compromise every Dialogflow CX agent within the same Google Cloud project.

Hackers exploit Roundcube flaw to spy on academic researchers

BleepingComputer - 08 July 2026 15:56

A China-linked threat cluster has been exploiting vulnerable Roundcube servers at U.S. and Canadian universities to steal credentials and deploy backdoor malware.

Ubiquiti Patches Critical UniFi Flaws Across Connect, Talk, Access, Protect, and OS

The Hacker News - 08 July 2026 21:08

Ubiquiti has shipped updates to address multiple critical security flaws impacting UniFi Connect, UniFi Talk, UniFi Access, UniFi Protect, and UniFi OS that could result in privilege escalation and arbitrary command execution. The list of vulnerabilities is as follows - CVE-2026-50746 (CVSS score: 10.0) - An improper access control vulnerability in UniFi Connect Application.

CISA Urges Immediate Patching of Exploited ColdFusion, Langflow, Joomla Flaws

SecurityWeek - 08 July 2026 11:45

Two newly disclosed critical vulnerabilities in Adobe ColdFusion and Langflow join two Joomla extension flaws in CISA’s Known Exploited Vulnerabilities catalog, with federal agencies given until July 10 to patch.

CISA Deploys Anthropic’s Mythos AI to Hunt Vulnerabilities in U.S. Government Code

Security Affairs - 08 July 2026 08:24

Three sources familiar with the matter told Reuters that CISA, the U.S. government’s civilian cyber defense agency, is running Anthropic’s Mythos AI model against federal code repositories to find vulnerabilities before foreign intelligence.

Scottish Cyber Coordination Centre

Threat actors and malware

Accenture Confirms Data Breach After Hacker Claims Source Code Theft

SecurityWeek - 08 July 2026 17:09

The professional services giant says it contained the incident, remediated its source, and experienced no operational or service delivery impact.

Telegram-Hosted RedWing Malware Lets Anyone Rent Android Spyware Tools

Security Affairs - 08 July 2026 12:09

Zimperium's zLabs team has uncovered RedWing, an Android spyware operation sold as a subscription service through Telegram, with links to Russian threat actors and apparent roots in the Oblivion malware family.

New HalluSquatting Attack Could Trick AI Coding Assistants Into Installing Botnet Malware

The Hacker News - 08 July 2026 21:37

AI coding assistants have a habit of making things up. Ask one to fetch a popular tool, and it will sometimes hand back a real-sounding name for a project that does not exist. New research, which its authors call HalluSquatting, turns that habit into an attack.

China-Linked UAT-7810 Expands ORB Network With New LONGLEASH Malware

The Hacker News - 08 July 2026 15:34

A Chinese threat actor tracked as UAT-7810 is actively refining its bespoke malware to expand its Operational Relay Box (ORB) network by breaking into internet-facing networking devices.

New Ghost Phishing Wave Is Breaking Traditional Email Security

The Hacker News - 08 July 2026 19:30

A recent EvilTokens campaign targeting businesses across the US and Europe is exposing a new email security blind spot. This "ghost phishing" technique keeps the malicious page hidden until it decrypts and comes to life inside the victim's browser.