Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 July 2026

Vulnerabilities

Fourth SharePoint Vulnerability Exploited in Past Month's Wave of Attacks

SecurityWeek - 22 July 2026 12:29

CVE-2026-50522 is being exploited by threat actors to steal machine keys and retain long-term access.

Adobe Chrome extension flaw let sites access private WhatsApp chats

BleepingComputer - 22 July 2026 10:22

The Adobe Acrobat extension for Chrome could be used to access conversations and data rendered in WhatsApp Web without any form of authentication.

CVE-2026-8933: Ubuntu security flaw breaks Snap sandbox protections

Security Affairs - 22 July 2026 23:25

Qualys has disclosed a high-severity local privilege escalation vulnerability, tracked as CVE-2026-8933 (CVSS score of 7.8), affecting default installations of Ubuntu Desktop 24.04, 25.10, and 26.04.

New InfraTrust report reveals infrastructure flaws admins should patch first

BleepingComputer - 22 July 2026 11:15

Eclypsium has launched InfraTrust, a new infrastructure cybersecurity knowledge base and monthly InfraTrust Pulse report designed to help organizations prioritize vulnerabilities affecting infrastructure, firmware, networking, and edge devices.

Hackers Exploit Windmill Flaw to Read Arbitrary Server Files Without Authentication

The Hacker News - 22 July 2026 19:06

A high-severity security flaw impacting open-source developer platform Windmill has come under active exploitation in the wild, per VulnCheck. The vulnerability in question is CVE-2026-29059 (CVSS score: 7.5), a case of unauthenticated path traversal impacting Windmill's "get_log_file" endpoint ("/api/w/{workspace}/jobs_u/get_log_file/{filename}").

Oracle Patches Over 1,400 Vulnerabilities With Quarterly Security Updates

SecurityWeek - 22 July 2026 10:33

Many of the vulnerabilities fixed with the July 2026 Critical Patch Update were likely discovered by AI.

Scottish Cyber Coordination Centre

Threat actors and malware

OpenAI Says Its AI Models Escaped Sandbox, Targeted Hugging Face to Cheat Benchmark

The Hacker News - 22 July 2026 18:00

OpenAI on Tuesday said a combination of its artificial intelligence (AI) models, including GPT-5.6 Sol and an “even more capable pre-release model,” was behind the security incident that targeted Hugging Face’s production infrastructure last week.

Police Dismantle Kratos Phishing Kit Built to Steal Microsoft 365 Sessions and Bypass MFA

The Hacker News - 22 July 2026 13:08

German and US law enforcement have taken down the core infrastructure of Kratos, described by German investigators as one of the world’s most widely used criminal phishing kits, and Indonesian authorities arrested the man they say developed and ran it.

US Warns of Iranian Hackers Targeting Siemens, Schneider, and Rockwell ICS Devices

SecurityWeek - 23 July 2026 06:28

An updated advisory from federal agencies provides information on the techniques used to hack programmable logic controllers.