Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 June 2026

Vulnerabilities

Microsoft fixes AutoGen Studio flaw that enabled code execution

BleepingComputer - 22 June 2026 14:28

A vulnerability chain dubbed AutoJack in Microsoft's AutoGen Studio interface for prototyping AI agents could let attackers manipulate an agent into executing arbitrary commands on its host system simply by visiting a malicious webpage.

29-Year-Old Squid Proxy Bug 'Squidbleed' Can Leak Cleartext HTTP Requests

The Hacker News - 22 June 2026 20:59

A heap over-read in the Squid web proxy can leak another user's cleartext HTTP request, including any credentials or session tokens it carries, to anyone already allowed to send traffic through the same proxy.

New Exploit Bypasses Apple's Boot Defenses, Affects Millions of iPhones

SecurityWeek - 22 June 2026 11:03

The vulnerability exploited by the Usbliter8 exploit cannot be patched and a PoC exploit has been released by researchers.

Attackers Exploit Gravity SMTP Plugin Flaw to Harvest Valuable WordPress Data

SecurityWeek - 22 June 2026 12:45

Vulnerable WordPress plugin iterations leak API keys, secrets, tokens, server information, and other data.

FFmpeg fixes PixelSmash flaw in widely used video decoder

BleepingComputer - 22 June 2026 18:05

A newly disclosed FFmpeg flaw dubbed 'PixelSmash' could be exploited for remote code execution on Jellyfin servers under certain conditions, and can also trigger a denial-of-service condition in applications like Kodi, Emby, Nextcloud, PhotoPrism, and OBS Studio.

OpenAI Expands Daybreak With GPT-5.5-Cyber to Help Defenders Patch Security Flaws

The Hacker News - 23 June 2026 10:26

OpenAI on Monday said it's releasing an improved version of its GPT-5.5-Cyber model to trusted defenders as part of the Daybreak initiative the artificial intelligence (AI) company announced last month.

Scottish Cyber Coordination Centre

Threat actors and malware

FortiBleed: The Most Detailed Breakdown Yet of an Active Russian Credential-Harvesting Operation

Security Affairs - 22 June 2026 11:25

FortiBleed targeted 430,000+ FortiGate devices, harvesting 110M credentials and enabling breaches through large-scale credential theft.

WhatsApp phishing attack uses fake business docs to hack PCs

BleepingComputer - 22 June 2026 19:42

An ongoing malware campaign is targeting WhatsApp users in multiple countries with deceptive messages that push VBScript files, leading to remote system access.

AryStinger Malware Infects 4,300 Legacy Routers to Build Reconnaissance Proxy Network

The Hacker News - 22 June 2026 13:27

A new malware family is turning forgotten home routers into a distributed reconnaissance and proxy network, not the DDoS botnet these devices usually end up in.

Microsoft Attributes Mastra AI Supply Chain Attack to North Korea

Infosecurity Magazine - 22 June 2026 12:30

North Korean threat actor Sapphire Sleet has been linked to a supply chain attack targeting Mastra, according to Microsoft security researchers.

What the Latest ShinyHunters Breaches Reveal About Modern Cyberattacks

SecurityWeek - 22 June 2026 11:30

Groups like ShinyHunters are demonstrating that attackers do not necessarily need malware or zero-day exploits to cause massive damage.