Scottish Cyber Coordination Centre

Daily Threat Bulletin

14 July 2026

Vulnerabilities

CISA warns of actively exploited RCE flaws in Joomla extensions

BleepingComputer - 13 July 2026 12:20

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning that attackers are exploiting vulnerabilities in the iCagenda and Balbooa Forms extensions for Joomla to achieve remote code execution through arbitrary file uploads. [...]

U.S. CISA adds a Cisco IOS flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 13 July 2026 19:05

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a Cisco IOS flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Cisco IOS flaw, tracked as CVE-2008-4128, to its Known Exploited Vulnerabilities (KEV) catalog.

Australia Alerts Organizations to Ongoing CMS Exploitation Attacks

Security Affairs - 13 July 2026 08:39

Australia warns of a global campaign exploiting CMS flaws to deploy webshells on WordPress, Joomla, and other websites.

RabbitMQ Vulnerability Threatens Enterprise Systems

SecurityWeek - 13 July 2026 13:00

Unauthenticated attackers could obtain the broker's confidential OAuth client secret, allowing them to take control of the broker.

Zimbra Patches Critical Code Execution Vulnerability

SecurityWeek - 13 July 2026 11:03

The flaw results in malicious code embedded in crafted emails being executed when the emails are opened.

Threat actors and malware

CC-4812 - Progress Software Addresses a Security Threat to ShareFile Storage Zone Controllers

NHS Digital - 13 July 2026 12:45

Scottish Cyber Coordination Centre

Severity: Medium Progress Software urgers customers to manually shut down Windows servers hosting Storage Zone Controllers Progress Software urgers customers to manually shut down Windows servers hosting Storage Zone Controllers Updated: 13 Jul 2026

Hackers backdoor Jscrambler npm package with infostealer malware

BleepingComputer - 13 July 2026 16:44

The Jscrambler client-side web security company disclosed that a threat actor published a malicious version of its npm package that has been downloaded almost 1,500 times. [...]

CrashStealer macOS Malware Uses Notarized Dropper to Pass Gatekeeper Checks

The Hacker News - 14 July 2026 00:06

Cybersecurity researchers have flagged a new macOS information stealer called CrashStealer that's capable of harvesting sensitive data from compromised systems.Unlike other information stealers that are built on AppleScript droppers or Objective-C-based wrappers, CrashStealer is implemented in native C++, according to Jamf Threat Labs.

Forg365 PhaaS Targets Microsoft 365 with Device Code and AitM Session Theft

The Hacker News - 13 July 2026 19:33

A new phishing-as-a-service (PhaaS) operation called Forg365 is using a combination of device code phishing, adversary-in-the-middle (AitM) tactics, antibot evasion, artificial intelligence (AI)-assisted lure creation, and post-compromise mailbox operations targeting Microsoft 365 accounts.

Misconfigured Server Reveals Three Evilginx Phishing Operations Targeting Microsoft 365

The Hacker News - 13 July 2026 14:00

An attacker running a live Microsoft 365 phishing operation left a Python web server listening on a public port with directory listing switched on.

GigaWiper Lets Threat Actors Choose Their Own Destructive Attack

darkreading - 13 July 2026 17:50

A modular implant borrows from various malware families to combine both backdoor and wiper activities to maximize impact and minimize operational output.

UK related

UK and Allies urge critical sectors to improve defences against Russian intelligence targeting

NCSC - 13 July 2026 13:00

New advisory highlights Russian state cyber actors' global exploitation of poorly configured routers

Scottish Cyber Coordination Centre

UK charges suspects linked to Russian Coms call spoofing platform

BleepingComputer - 13 July 2026 10:23

UK authorities charged five people following a National Crime Agency (NCA) investigation into Russian Coms, a major caller ID spoofing platform used by criminals to make over 1.8 million scam calls. [...]