Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 July 2026

Vulnerabilities

Attackers actively exploit the Oracle E-Business Suite flaw CVE-2026-46817

Security Affairs - 30 June 2026 10:01

Attackers are exploiting a critical flaw in Oracle E-Business Suite, CVE-2026-46817, that allows remote, unauthenticated attackers to take over Oracle Payments.

Attackers Exploit SimpleHelp CVE-2026-48558 to Deploy TaskWeaver and Djinn Stealer

The Hacker News - 30 June 2026 17:48

An unknown threat actor has been observed exploiting a recently disclosed maximum-severity security flaw in SimpleHelp to deliver two previously unreported malware families, TaskWeaver and Djinn Stealer.

BlueHammer Vulnerability Exploited in Ransomware Attacks

SecurityWeek - 30 June 2026 14:56

The Microsoft Defender vulnerability CVE-2026-33825 was exploited in the wild as a zero-day before patches were released.

Progress Kemp LoadMaster Flaw Could Let Attackers Run Root Commands Pre-Auth

The Hacker News - 30 June 2026 14:08

A critical vulnerability in Progress Kemp LoadMaster can let an unauthenticated attacker execute arbitrary commands as root on the appliance by sending a crafted request to its API. The flaw, tracked as CVE-2026-8037, carries a CVSS score of 9.8 according to ZDI. A patch is available.

Citrix Patches Six NetScaler Flaws Allowing File Read and Denial-of-Service

The Hacker News - 01 July 2026 10:24

Citrix on Tuesday released security updates to address multiple flaws in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) that could be exploited by an attacker to facilitate arbitrary file reads or trigger a denial-of-service (DoS) condition.

Google Patches 382 Chrome Vulnerabilities

SecurityWeek - 01 July 2026 07:14

Fifteen of the newly patched flaws have been rated ‘critical’ and 67 have been rated ‘high severity’.

Scottish Cyber Coordination Centre

Apple Fixes WebKit Flaws in iOS and macOS, With Help From AI Tools

Security Affairs - 30 June 2026 12:32

Apple released updates for iOS, iPadOS, macOS, and Safari, fixing WebKit flaws, four of which were found using AI tools like Claude and Codex.

Threat actors and malware

New BioShocking attack manipulates AI browser into data theft

BleepingComputer - 30 June 2026 18:50

A new prompt injection attack dubbed “BioShocking” could trick AI-powered browsers into treating real-world risky actions as part of a fictional scenario, causing them to ignore any safety guardrails.

Researcher Analyzes 3,000 Live ClickFix Payloads, Exposing API-Driven Malware Delivery

The Hacker News - 01 July 2026 12:02

ClickFix, the trick that fools people into running malware by hand, has quietly grown a back office. New research shows the malicious commands behind its fake “prove you’re human” pages are now handed out by API-driven servers that give each visitor the same malware in a different disguise.

AirDrop and Quick Share Flaws Let Nearby Attackers Trigger Crashes and Bypass Checks

The Hacker News - 30 June 2026 15:57

Two researchers have found six security flaws in AirDrop and Quick Share, the wireless features that beam files between nearby devices with no cables or shared network.

UK incidents

UK Healthcare Sector Records Tenfold Increase in Cyber-Attacks

Infosecurity Magazine - 30 June 2026 10:30

SonicWall records 264,000 events in first five months of 2026 as UK hospitals come under siege.

Over 300 UK Firms Hit by Ransomware in a Year

Infosecurity Magazine - 30 June 2026 09:00

Report Fraud data reveals that more than half of 323 UK ransomware victims last year were SMEs.