Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 July 2026

Vulnerabilities

Oracle E-Business Suite Flaw Under Active Attack, 950 Systems Exposed

Security Affairs - 01 July 2026 20:49

This week, Defused Cyber researchers warned that a critical vulnerability in Oracle E-Business Suite, tracked as CVE-2026-46817, is being actively exploited. The flaw affects Oracle Payments versions 12.2.3 through 12.2.15.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2026-45659 Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability

Progress Kemp LoadMaster Pre-Auth RCE Flaw Faces Active Exploitation Attempts

The Hacker News - 01 July 2026 20:26

A recently disclosed critical security flaw impacting Progress Kemp LoadMaster is seeing active exploitation attempts, according to an advisory from eSentire's Threat Response Unit (TRU).

Critical Cursor Flaws Could Let Prompt Injection Escape Sandbox and Run Commands

The Hacker News - 01 July 2026 21:12

Two flaws in Cursor, an AI code editor, could let a single, ordinary-looking prompt break out of the editor's safety sandbox and run any command on a developer's computer. There is no click to fall for and no approval box to ignore.

Unpatched Argo CD Repo-Server Flaw Could Let Attackers Take Over Kubernetes Clusters

The Hacker News - 02 July 2026 02:10

Argo CD, a widely used tool for deploying software to Kubernetes, has an unpatched flaw in its repo-server component that lets an unauthenticated attacker run code, provided they can reach the component's internal network port.

Scottish Cyber Coordination Centre

Adobe Patches Critical ColdFusion, Campaign Classic Vulnerabilities

SecurityWeek - 01 July 2026 12:27

Seven of the security defects have a maximum severity rating of 10/10 and could lead to arbitrary code execution.

Citrix Patches NetScaler Vulnerabilities, Including New 'HTTP/2 Bomb' Attack

SecurityWeek - 01 July 2026 12:20

Citrix urges customers to patch NetScaler after fixing six vulnerabilities, including the HTTP/2 Bomb flaw and a high-severity CitrixBleed-style information disclosure bug.

Apple Patches Dozens of Vulnerabilities Across iOS, macOS, and Safari

SecurityWeek - 01 July 2026 10:30

The updates fix vulnerabilities in WebKit, the kernel, WebRTC, Web Extensions, and other components affecting iPhone, iPad, Mac, and Safari users.

Threat actors and malware

FortiBleed credential-theft campaign linked to Lynx ransomware

BleepingComputer - 01 July 2026 18:37

The massive FortiBleed credential theft campaign has been linked to the INC and Lynx ransomware operations, suggesting the stolen Fortinet credentials were intended to fuel future network intrusions.

New ChocoPoC malware targets researchers via trojanized PoC exploits

BleepingComputer - 01 July 2026 17:08

Multiple weaponized proof-of-concept (PoC) exploits on GitHub were found delivering a Python-based remote access trojan (RAT) named ChocoPoC that can execute commands and steal sensitive data in a campaign believed to target cybersecurity researchers.

Hackers target Microsoft 365 accounts with 81 million login attempts

BleepingComputer - 01 July 2026 13:38

An aggressive password-spraying campaign targeting Microsoft 365 environments generated more than 81 million login attempts over a two-week period.

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

The Hacker News - 01 July 2026 12:02

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.