Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 July 2026

Vulnerabilities

Claude Chrome extension flaw lets malicious extensions trigger AI actions

BleepingComputer - 16 July 2026 16:26

A flaw in Anthropic's Claude for Chrome browser extension could allow a malicious extension to trigger predefined AI actions by simulating user clicks, potentially allowing it to abuse Claude's access to connected services such as Gmail, Google Docs, Google Calendar, and Salesforce.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-25089 Fortinet FortiSandbox OS Command Injection Vulnerability

CVE-2026-39808 Fortinet FortiSandbox OS Command Injection Vulnerability

CVE-2026-58644 Microsoft SharePoint Deserialization of Untrusted Data Vulnerability

CISA orders feds to patch actively exploited Oracle flaw by Saturday

BleepingComputer - 16 July 2026 07:56

CISA has ordered federal agencies to secure their systems by Saturday against ongoing attacks exploiting a critical vulnerability in the Oracle E-Business Suite financial application.

Zoom Fixes CVE-2026-53412, a Critical Account Takeover Bug

Security Affairs - 16 July 2026 08:36

Zoom has fixed a critical Windows vulnerability, tracked as CVE-2026-53412 (CVSS score of 9.8) that could allow unauthenticated attackers to hijack user accounts.

F5 Patches Multiple NGINX, BIG-IP Vulnerabilities

SecurityWeek - 16 July 2026 10:20

Attackers could exploit the bugs to modify configurations, terminate or restart processes, cross security boundaries, leak memory, and execute code.

Scottish Cyber Coordination Centre

Threat actors and malware

New ClickLock macOS malware traps users into revealing login password

BleepingComputer - 16 July 2026 18:52

A new macOS information-stealing malware dubbed ClickLock terminates all visible processes to force users into entering their system login password.

New TELEPUZ Malware Spreads via ClickFix to Steal Data and Run Commands

The Hacker News - 16 July 2026 19:20

Cybersecurity researchers have called attention to a new modular malware called TELEPUZ that's been spreading via websites infected with ClickFix lures since late April 2026.

UK incidents

Two Scattered Spider Hackers Sentenced to Jail in UK

SecurityWeek - 16 July 2026 14:21

Thalha Jubair and Owen Flowers were prosecuted over a 2024 cyberattack targeting Transport for London (TfL).