Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 July 2026

Vulnerabilities

Cisco finally confirms attackers exploiting Unified CM flaw

BleepingComputer - 02 July 2026 08:35

Cisco confirmed that attackers are now exploiting a Unified Communications Manager (Unified CM) vulnerability patched in early June.

U.S. CISA adds a Microsoft SharePoint Server flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 02 July 2026 16:56

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Microsoft SharePoint Server flaw, tracked as CVE-2026-45659 (CVSS score v3.1 of 8.8), to its Known Exploited Vulnerabilities (KEV) catalog.

New CitrixBleed Vulnerability Exploited Immediately After Public Disclosure

SecurityWeek - 02 July 2026 16:04

Hackers are targeting NetScaler appliances using public PoC code to retrieve arbitrary memory content in the HTTP response.

Adobe fixed multiple maximum-severity flaws in ColdFusion and Campaign Classic

Security Affairs - 02 July 2026 10:21

Adobe fixed multiple critical flaws, including max severity bugs in ColdFusion and Campaign Classic that could lead to remote code execution Adobe has released security updates for ColdFusion and Campaign Classic, fixing multiple critical vulnerabilities, including seven maximum-severity issues (CVSS score of 10.0).

CC-4807 - Critical Vulnerabilities in UltraVNC Repeater Component

NHS Digital - 02 July 2026 15:18

Severity: Medium The critical vulnerabilities could allow a remote attacker either to obtain administrative control of the service through a hard-coded credential (CVE-2026-7839) or achieve unauthenticated arbitrary code execution (CVE-2026-7840).

Scottish Cyber Coordination Centre

Threat actors and malware

FortiBleed Campaign Linked to INC, Lynx Ransomware Attacks

SecurityWeek - 02 July 2026 13:34

Researchers say credentials harvested from hundreds of thousands of FortiGate firewalls are being used to facilitate ransomware attacks by the INC and Lynx operations.

Ransomware Groups Turn to Citrix Bleed 2, BYOVD, and Supply Chain Credentials

The Hacker News - 03 July 2026 01:00

Threat actors associated with the Anubis ransomware operation have been observed exploiting the Citrix Bleed 2 (CVE-2025-5777) vulnerability to obtain initial access. Although tactics differ between affiliates, common patterns emerged in tradecraft through use of legitimate Remote Management and Monitoring (RMM) tooling, credential access, and hands-on-keyboard procedures

ToddyCat-Linked Umbrij Malware Abuses OAuth to Access Gmail via Google API

The Hacker News - 02 July 2026 19:34

The threat actor known as ToddyCat has been attributed to a new malware called Umbrij that's designed to gain surreptitious access to a victim's email correspondence via the Google API.

Fake Google and Cloudflare verification pages spread multiple malware families

Malwarebytes - 02 July 2026 17:05

We uncovered ClickFix attacks using fake Google and Cloudflare pages to deliver everything from infostealers to a newly discovered malware loader.

Opera rolls out Paste Protect feature to fight ClickFix attacks

BleepingComputer - 02 July 2026 07:46

Opera has introduced Paste Protect, a security feature designed to block ClickFix-style attacks that trick users into executing malicious commands through social engineering.