Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

8 July 2025

Vulnerabilities

Public exploits released for Citrix Bleed 2 NetScaler flaw, patch now

BleepingComputer - 07 July 2025 19:57

Researchers have released proof-of-concept (PoC) exploits for a critical Citrix NetScaler vulnerability, tracked as CVE-2025-5777 and dubbed CitrixBleed2, warning that the flaw is easily exploitable and can successfully steal user session tokens. [...]

U.S. CISA adds Google Chromium V8 flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 07 July 2025 08:14

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Chromium V8 vulnerability to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Chromium V8 vulnerability, tracked as CVE-2025-6554, to its Known Exploited Vulnerabilities (KEV) catalog.

⚡ Weekly Recap: Chrome 0-Day, Ivanti Exploits, MacOS Stealers, Crypto Heists and More

The Hacker News - 07 July 2025 17:56

Everything feels secure—until one small thing slips through. Even strong systems can break if a simple check is missed or a trusted tool is misused. Most threats don't start with alarms—they sneak in through the little things we overlook.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2014-3931 Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability; CVE-2016-10033 PHPMailer Command Injection Vulnerability; CVE-2019-5418 Rails Ruby on Rails Path Traversal VulnerabilityCVE-2019-9621 Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability.

Threat actors and malware

Atomic macOS infostealer adds backdoor for persistent attacks

BleepingComputer - 07 July 2025 15:24

Malware analyst discovered a new version of the Atomic macOS info-stealer (also known as 'AMOS') that comes with a backdoor, to attackers persistent access to compromised systems. [...]

Hackers abuse leaked Shellter red team tool to deploy infostealers

BleepingComputer - 07 July 2025 11:49

Shellter Project, the vendor of a commercial AV/EDR evasion loader for penetration testing, confirmed that hackers used its Shellter Elite product in attacks after a customer leaked a copy of the software. [...]

New Batavia spyware targets Russian industrial enterprises

Security Affairs - 07 July 2025 19:22

Since March 2025, fake contract emails have been spreading Batavia spyware in targeted attacks on Russian organizations. Since March 2025, a targeted phishing campaign against Russian organizations has used fake contract-themed emails to spread the Batavia spyware, a new malware designed to steal internal documents.

SEO Poisoning Campaign Targets 8,500+ SMB Users with Malware Disguised as AI Tools

The Hacker News - 07 July 2025 23:56

Cybersecurity researchers have disclosed a malicious campaign that leverages search engine optimization (SEO) poisoning techniques to deliver a known malware loader called Oyster (aka Broomstick or CleanUpLoader).

TAG-140 Targets Indian Government Via 'ClickFix-Style' Lure

darkreading - 08 July 2025 04:30

The threat actors trick victims into opening a malicious script, leading to the execution of the BroaderAspect .NET loader.