



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

8 October 2026

Vulnerabilities

Hackers exploit critical Atlassian flaw after public PoC release

BleepingComputer - 07 October 2026 09:49

A critical vulnerability (CVE-2026-21589) affecting multiple Atlassian product families, including Jira, Confluence, and Bitbucket, is being exploited in attacks that do not require authentication.

FortiBleed hit 86,000 firewalls by exploiting something nobody can patch away

Security Affairs - 07 October 2026 14:49

FBI and Secret Service warn FortiBleed, a credential-harvesting campaign against Fortinet firewalls, has compromised 86,644 devices and is locking out admins.

SonicWall Patches CVSS 10.0 Pre-Authentication SSRF Flaw in SMA1000 Appliances

The Hacker News - 07 October 2026 22:47

SonicWall has released hotfixes for four flaws in its SMA1000 appliances, the gateways that give remote workers access to a company's network and applications. The most serious could allow an attacker without a login to send requests through the appliance and reach internal functions.

Unpatched Critical LMCache Flaw Lets Unauthenticated Attackers Run Code Remotely

The Hacker News - 07 October 2026 22:04

A critical vulnerability in LMCache, open-source software that speeds up large language model (LLM) servers such as vLLM, lets an attacker run code on the cache server without logging in, and no fixed version is available. The flaw is in LMCache's multiprocess mode, where the cache runs as a standalone server that LLM workers reach over the ZeroMQ messaging library.

Chrome 155 Update Patches 247 Vulnerabilities

SecurityWeek - 07 October 2026 11:51

Four critical-severity use-after-free defects were fixed in Chromecast, Browser, Navigation, and Track.



Scottish
Cyber
Coordination
Centre

Android's October 2026 Updates Patch 25 Vulnerabilities

SecurityWeek - 07 October 2026 07:55

The patches resolve a critical vulnerability in Android's System component that could lead to privilege escalation.

Threat actors and malware

Hackers hijack Google domains after breaching ccTLD registries

BleepingComputer - 07 October 2026 17:50

Hackers obtained unauthorized HTTPS certificates for several Google domains and hijacked domains in the country-code top-level domains (ccTLDs) for Ghana, American Samoa, and Sierra Leone after compromising third-party operators and modifying authoritative DNS records.

CERT-UA: Fake Cloudflare Checks Deliver LunexStealer Malware

Security Affairs - 07 October 2026 14:22

Over 100 hacked websites used fake Cloudflare checks to trick visitors into installing LunexStealer through ClickFix commands. The lure is the now-familiar ClickFix technique, dressed up as Cloudflare's standard bot check.

Samsung Galaxy S26 hacked three more times at Pwn2Own Ireland

BleepingComputer - 08 October 2026 03:32

On the second day of Pwn2Own Ireland 2026, security researchers collected \$232,500 in cash awards after exploiting 45 unique zero-day vulnerabilities.

Qilin Ransomware Suspect Arrested in Japan, Extradited to Germany

SecurityWeek - 07 October 2026 14:47

The individual was detained in May and has been extradited to Germany to face hacking charges.

ASOS Confirms Cyberattack, Data Breach

SecurityWeek - 07 October 2026 10:46

Hackers compromised a third-party communication platform and sent rogue notifications to ASOS users.