Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 September 2025

Vulnerabilities

Libraesva ESG issues emergency fix for bug exploited by state hackers

BleepingComputer - 23 September 2025 14:51

Libraesva rolled out an emergency update for its Email Security Gateway solution to fix a vulnerability exploited by threat actors believed to be state sponsored. [...]

CISA says hackers breached federal agency using GeoServer exploit

BleepingComputer - 23 September 2025 12:07

CISA has revealed that attackers breached the network of an unnamed U.S. federal civilian executive branch (FCEB) agency last year after compromising an unpatched GeoServer instance. [...]

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

Security Affairs - 23 September 2025 19:50

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Google Chromium flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chromium flaw, tracked as CVE-2025-10585, to its Known Exploited Vulnerabilities (KEV) catalog.

SolarWinds Releases Hotfix for Critical CVE-2025-26399 Remote Code Execution Flaw

The Hacker News - 23 September 2025 19:16

SolarWinds has released hot fixes to address a critical security flaw impacting its Web Help Desk software that, if successfully exploited, could allow attackers to execute arbitrary commands on susceptible systems.

Patch Bypassed for Supermicro Vulnerability Allowing BMC Hack

SecurityWeek - 23 September 2025 19:00

Binarly researchers have found a way to bypass a patch for a previously disclosed vulnerability.

Threat actors and malware

SonicWall releases SMA100 firmware update to wipe rootkit malware

BleepingComputer - 23 September 2025 10:15

SonicWall has released a firmware update that can help customers remove rootkit malware deployed in attacks targeting SMA 100 series devices. [...]

BadIIS Malware Spreads via SEO Poisoning — Redirects Traffic, Plants Web Shells

The Hacker News - 23 September 2025 14:43

Cybersecurity researchers are calling attention to a search engine optimization (SEO) poisoning campaign likely undertaken by a Chinese-speaking threat actor using a malware called BadIIS in attacks targeting East and Southeast Asia, particularly with a focus on Vietnam.

Disabling Hospital HVAC Is Now a Bargaining Chip in Ransomware

Security Magazine - 24 September 2025 02:00

Shutting down a hospital's heating and cooling system would be a patient safety disaster.

GitHub moves to tighten npm security amid phishing, malware plague

The Register - 23 September 2025 14:18

Hundreds of compromised packages pulled as registry shifts to 2FA and trusted publishing GitHub, which owns the npm registry for JavaScript packages, says it is tightening security in response to recent attacks....

Suspected Iran-backed attackers targeting European aerospace sector with novel malware

The Register - 23 September 2025 11:52

Instead of job offers, victims get MiniJunk backdoor and MiniBrowse stealer Suspected Iranian government-backed online attackers have expanded their European cyber ops with fake job portals and new malware targeting organizations in the defense, manufacturing, telecommunications, and aviation sectors....

A Massive Telecom Threat Was Stopped Right As World Leaders Gathered at UN Headquarters in New York

SecurityWeek - 23 September 2025 23:30

More than 300 servers and 100,000 SIM cards designed to mimic cellphones and overwhelm networks.

All Microsoft Entra Tenants Were Exposed to Silent Compromise via Invisible Actor Tokens: Researcher

SecurityWeek - 23 September 2025 12:44

The strength of responsible disclosure is that it can solve problems before they are actioned. The weakness is that it potentially generates a false sense of security in the vendor.

UK related

Scottish Cyber Coordination Centre

UK chancellor Putin the blame on Russia for cyber chaos, but evidence says otherwise

The Register - 23 September 2025 11:07

Reeves points finger at Moscow in interview when authorities reckon it's local lads UK chancellor Rachel Reeves is blaming Moscow for Britain's latest cyber woes, an attribution that seems about as solid as wet cardboard given the trail of evidence pointing to attackers much closer to home....

Jaguar Land Rover Says Shutdown Will Continue Until at Least Oct 1 After Cyberattack

SecurityWeek - 23 September 2025 23:39

JLR extended the pause in production "to give clarity for the coming week as we build the timeline for the phased restart of our operations and continue our investigation.