Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 August 2025

Vulnerabilities

Proton fixes Authenticator bug leaking TOTP secrets in logs

BleepingComputer - 04 August 2025 16:09

Proton fixed a bug in its new Authenticator app for iOS that logged users' sensitive TOTP secrets in plaintext, potentially exposing multi-factor authentication codes if the logs were shared. [...]

NVIDIA Triton Bugs Let Unauthenticated Attackers Execute Code and Hijack AI Servers

The Hacker News - 04 August 2025 22:36

A newly disclosed set of security flaws in NVIDIA's Triton Inference Server for Windows and Linux, an open-source platform for running artificial intelligence (AI) models at scale, could be exploited to take over susceptible servers."When chained together, these flaws can potentially allow a remote, unauthenticated attacker to gain complete control of the server, achieving remote code execution

Nvidia Patches Critical RCE Vulnerability Chain

darkreading - 04 August 2025 21:53

The flaws in the company's Triton Inference Server enables model theft, data leaks, and response manipulation.

Several Vulnerabilities Patched in AI Code Editor Cursor

SecurityWeek - 04 August 2025 09:50

Attackers could silently modify sensitive MCP files to trigger the execution of arbitrary code without requiring user approval.

Threat actors and malware

New Plague Linux malware stealthily maintains SSH access

BleepingComputer - 04 August 2025 11:42

A newly discovered Linux malware, which has evaded detection for over a year, allows attackers to gain persistent SSH access and bypass authentication on compromised systems. [...]

Ransomware gangs join attacks targeting Microsoft SharePoint servers

BleepingComputer - 04 August 2025 08:26

Ransomware gangs have recently joined ongoing attacks targeting a Microsoft SharePoint vulnerability chain, part of a broader exploitation campaign that has already led to the breach of at least 148 organizations worldwide. [...]

SonicWall Investigating Potential SSL VPN Zero-Day After 20+ Targeted Attacks Reported

The Hacker News - 05 August 2025 11:48

SonicWall said it's actively investigating reports to determine if there is a new zero-day vulnerability following reports of a spike in Akira ransomware actors in late July 2025.

UK related

Millions of age checks performed as UK Online Safey Act gets rolling

The Register - 04 August 2025 10:15

But it's OK, claims Brit government, no personal data stored 'unless absolutely necessary' The UK government has reported that an additional five million age checks are being made daily as UK-based internet users seek to access age-restricted sites following the implementation of the Online Safety Act."