Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 August 2026

Vulnerabilities

CC-4823 - Active Exploitation of Critical N-central Authentication Bypass Vulnerability

NHS Digital - 03 August 2026 11:17

Severity: Medium Exploitation of CVE-2026-18577 could allow an attacker to bypass authentication and lead to administrative account takeover Exploitation of CVE-2026-18577 could allow an attacker to bypass authentication and lead to administrative account takeover Updated: 03 Aug 2026

Hugging Face Diffusers Flaws Could Let Model Repositories Execute Arbitrary Code

The Hacker News - 03 August 2026 12:10

Three high-severity security flaws have been disclosed in Hugging Face's Diffusers library that could allow crafted model repositories to stealthily execute arbitrary code on machines that load it, opening the artificial intelligence (AI) supply chain to security risk."These vulnerabilities are bypassing trust_remote_code, the safeguard designed to stop unreviewed code from running in the

Internet-Facing SonicWall SMA Appliances Face Zero-Click Root Compromise

Cyber Security News - 03 August 2026 08:45

Internet-facing SonicWall Secure Mobile Access, or SMA, appliances face a serious threat after attackers turned two flaws into a route to full VPN-gateway control. The campaign gives an outsider a way to move from a simple web request to root-level access, without a password, session or user interaction. The activity began before public disclosure and [...]The post

Threat actors and malware

Chinese Threat Actor Uses Leaked DarkSword Kit to Deploy GHOSTBLADE on iOS

The Hacker News - 03 August 2026 16:19

An unknown Chinese-threat actor has been observed running a campaign targeting Apple iOS devices by leveraging a publicly leaked version of the DarkSword exploit kit.Attack surface management platform Censys said it identified the threat actor running more than 100 web properties, most of which are fake Amazon Web Services (AWS) sign-in pages on a domain that also hosts the exploit toolkit."

AI is 'both the weapon and the target' in latest wave of cyberattacks

The Register - 03 August 2026 09:01

Scottish Cyber Coordination Centre

CrowdStrike tracks 89% surge in machine-assisted activity as patch windows shrink to 48 hours

ModernStealer Threat Actor Linked to Government and Defense Data-Leak Claims

Cyber Security News - 03 August 2026 11:05

ModernStealer is the name behind underground posts claiming to offer military, government, nuclear, and aerospace material. The posts appeared on dark web forums and Telegram, making a single alias a concern for public-sector and defence teams. The activity is not a confirmed malware campaign or proof that every named organization was breached. It involves alleged [...]The post

Hackers Exploit N-able N-central Flaw After Initial Fix Falls Short

HackRead - 03 August 2026 12:24

N-able says attackers bypassed N-central authentication, reached managed client devices and installed Cloudflare tunnels that survived server access revocation.

UK related

PNLD Breach Exposes U.K. Police and Government Contact Details on Dark Web

The Hacker News - 03 August 2026 14:43

The Police National Legal Database (PNLD) has confirmed that police, government and customer contact information was compromised and published on the dark web.The data included names, organisations and work email addresses belonging to police officers, police staff, criminal justice professionals, government partners and customers.The incident, identified on July 26, also exposed some names