Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 November 2025

Vulnerabilities

ASUS warns of new critical auth bypass flaw in AiCloud routers

BleepingComputer - 26 November 2025 07:41

ASUS has released new firmware to patch nine security vulnerabilities, including a critical authentication bypass flaw in routers with AiCloud enabled.

Microsoft to secure Entra ID sign-ins from script injection attacks

BleepingComputer - 26 November 2025 09:26

Starting in mid-to-late October 2026, Microsoft will enhance the security of the Entra ID authentication system against external script injection attacks.

Popular Forge library gets fix for signature verification bypass flaw

BleepingComputer - 26 November 2025 15:32

A vulnerability in the 'node-forge' package, a popular JavaScript cryptography library, could be exploited to bypass signature verifications by crafting data that appears valid.

Threat actors and malware

Shai-Hulud v2 Spreads From npm to Maven, as Campaign Exposes Thousands of Secrets

The Hacker News - 27 November 2025 00:38

The second wave of the Shai-Hulud supply chain attack has spilled over to the Maven ecosystem after compromising more than 830 packages in the npm registry. The Socket Research Team said it identified a Maven Central package named org.mvnpm:posthog-node:4.18.1 that embeds the same two components associated with Sha1-Hulud: the "setup_bun.js" loader and the main payload "bun_environment.js.

RomCom Uses SocGholish Fake Update Attacks to Deliver Mythic Agent Malware

The Hacker News - 26 November 2025 14:58

The threat actors behind a malware family known as RomCom targeted a U.S.-based civil engineering company via a JavaScript loader dubbed SocGholish to deliver the Mythic Agent.

Scottish Cyber Coordination Centre

Qilin Ransomware Turns South Korean MSP Breach Into 28-Victim 'Korean Leaks' Data Heist

The Hacker News - 26 November 2025 21:01

South Korea's financial sector has been targeted by what has been described as a sophisticated supply chain attack that led to the deployment of Qilin ransomware. This operation combined the capabilities of a major Ransomware-as-a-Service (RaaS) group, Qilin, with potential involvement from North Korean state-affiliated actors (Moonstone Sleet), leveraging Managed Service Provider (MSP) compromise as the initial access vector.

UK incidents

Multiple London councils faced a cyberattack

Security Affairs - 26 November 2025 15:59

A cyberattack struck multiple London councils, including Kensington & Chelsea and Westminster, which share IT systems. Officials say residents' data may have been compromised and have notified the UK Information Commissioner's Office.