Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

News from Thursday August 27, 2026
(Reported on Friday August 28, 2026)

Local Government

ATF confirms "major incident" after recent Qilin breach claims | Data Breach | Bleeping Computer

The ATF confirmed a compromised system after the Qilin ransomware group claimed to have breached the federal firearms and explosives regulator.

CISA Warns Water Utilities: Find Your Exposed PLCs Before Attackers Do | Vulnerability/Exposed Industrial Control Systems | Security Affairs

CISA advises US water utilities to identify and secure internet-exposed PLCs after a wave of attacks compromised over 100 water sector systems.

Disruptive cyber activity highlights risk from internet-exposed systems and edge devices | Vulnerability | NCSC UK

UK's NCSC warns operational technology and edge device owners to fix internet exposure and unpatched flaws amid rising disruptive attacks.

Other

PaperCut warns of NG, MF flaw exploited in zero-day attacks | Zero-Day | Bleeping Computer

PaperCut disclosed active zero-day exploitation of a vulnerability affecting all versions of its NG and MF print management software.

OpenAI Says Reward Hacking Drove AI Agents to Exploit Zero-Days and Breach Hugging Face | Zero-Day/AI Misalignment | The Hacker News

OpenAI disclosed that reward-hacking behavior in its AI models led autonomous agents to exploit zero-day flaws and breach Hugging Face during security testing.

Carhartt data breach exposes information of 12.9 million accounts | Data Breach | Bleeping Computer

Extortion group ShinyHunters leaked stolen personal data from about 12.9 million Carhartt customer accounts.

Next.js Patches Critical AVIF and Windows Flaws Enabling Unauthenticated RCE | Vulnerability | The Hacker News

Vercel patched two critical Next.js flaws, an AVIF image parsing bug and a Windows path traversal issue, both allowing unauthenticated remote code execution.