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 Tuesday August 11, 2026
(Reported on Wednesday August 12, 2026)

Local Government

NIST wants to overhaul its vulnerability database for the AI age | Vulnerability | CyberScoop

NIST is soliciting public feedback on redesigning the National Vulnerability Database to handle AI-driven threats and machine-scale vulnerability data.

Healthcare

Ransomware group hijacks hospital system's Facebook page amid ongoing cyberattack fallout | Ransomware | The Record

Ransomware actors seized control of a hospital system's Facebook page, threatening to leak 6TB of stolen sensitive patient records.

Data Breaches Reported by Sunshine Health; Health Payment Systems | Social Engineering | HIPAA Journal

Florida Medicaid insurer Sunshine Health disclosed a voice-phishing (vishing) attack that led to theft of patient health information.

Other

Cisco warns of ASA and FTD VPN flaw exploited to crash devices | Vulnerability | Bleeping Computer

Cisco disclosed active exploitation of a high-severity denial-of-service flaw in ASA and FTD VPN software that can remotely crash firewall devices.

Researchers Disclose AI-Assisted SharePoint Exploit Chain Reaching Unauthenticated RCE | Vulnerability | The Hacker News

Researchers used AI-assisted analysis to chain SharePoint flaws into an unauthenticated exploit granting full administrative access.

Wesco confirms security incident after ExfilSquad claims data theft | Data Breach | Bleeping Computer

Global supply chain distributor Wesco confirmed a cybersecurity incident after threat group ExfilSquad claimed to have stolen company data.

Researchers Built a Fake Crypto Startup and Hired Three Suspected North Korean IT Workers | Social Engineering | The Hacker News

Researchers ran a decoy crypto company to expose North Korean operatives posing as remote developers using fabricated identities.