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 Monday August 17, 2026
(Reported on Tuesday August 18, 2026)

Local Government

US FCC Weighs Chinese Transceiver Supply-Chain Crackdown | Supply Chain Security / Policy | GovInfoSecurity

The FCC is considering adding Chinese-made optical transceivers used in AI data centers to its Covered List, potentially restricting new models over concerns about foreign technology embedded in critical U.S. network infrastructure.

Financial Institutions

SafePal data breach impacts 39,798 customers, stolen info for sale | Data Breach / Cryptocurrency |Bleeping Computer

Cryptocurrency hardware wallet provider SafePal disclosed a breach affecting 39,798 customers after attackers exploited a vulnerability to steal customer order information, which a threat actor later offered for sale.

Healthcare

CareCloud Data Breach Affects 3.75 Million Individuals | Data Breach | HIPAA Journal

CareCloud disclosed that unauthorized access to an electronic health record environment exposed the protected health information of more than 3.75 million individuals, making it one of the year's largest healthcare data breaches.

Other

Critical GitLab GraphQL Flaw Could Let Unauthenticated Attackers Delete Public Projects | Vulnerability | The Hacker News

A critical GitLab GraphQL vulnerability, CVE-2026-19478, could allow unauthenticated attackers to remotely modify or delete public projects and user data on vulnerable self-managed installations.

Snowflake GitHub Actions Flaw Lets Crafted Issues Trigger Command Injection | CI/CD Vulnerability | The Hacker News

Researchers discovered a GitHub Actions workflow injection flaw in Snowflake's public .NET connector repository that could allow a crafted GitHub issue to execute commands in a workflow containing internal Jira credentials.

Forminator WordPress Flaw Can Enable Unauthenticated RCE via Malicious PHP Uploads | Vulnerability / Remote Code Execution | The Hacker News

A critical Forminator Forms vulnerability, CVE-2026-15748, could allow unauthenticated attackers to upload malicious PHP files and achieve remote code execution on vulnerable WordPress sites.

Cavern C2 Uses DNS and Google Apps Script to Blend Into Legitimate Traffic | Cyber Espionage / Command and Control | The Hacker News

Iran-linked hackers are using an evolving Cavern C2 framework that leverages DNS and Google Apps Script to disguise command-and-control communications as legitimate network traffic.
