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 20, 2026
(Reported on Friday August 21, 2026)

Local Government

CISA Orders Feds to Patch Actively Exploited TrueConf Server Flaws | Vulnerability / Active Exploitation | BleepingComputer

CISA ordered federal agencies to patch two actively exploited TrueConf Server vulnerabilities that can enable unauthenticated remote code execution, with agencies required to remediate affected systems by September 3.

Financial Institutions

Report: One-Quarter of Breaches Are Enabled by AI-Driven Attacks | AI-Enabled Cyberattacks / Social Engineering | KnowBe4

An IBM-commissioned study found that one in four breaches is now AI-enabled, with these incidents averaging approximately $6 million in costs and financial services and critical infrastructure among the most heavily targeted sectors.

Healthcare

SickKids Data Breach Exposes Employee and Job Applicant Info | Data Breach | BleepingComputer

The Hospital for Sick Children disclosed a data breach involving personal information belonging to employees and job applicants, demonstrating that healthcare cyber incidents can expose workforce information in addition to patient data.

Other

Researchers Social-Engineered Copilot Into Exposing Flaw | AI Security / Social Engineering | GovInfoSecurity

Security researchers demonstrated how Microsoft Copilot could be socially engineered into revealing information associated with a security flaw, highlighting emerging risks when AI assistants interact with sensitive data and application functionality.

Hackers Abuse FTP Server Banners to Deliver New Windows Malware | Malware / Remote Access Trojan | BleepingComputer

Attackers are hiding commands in FTP server banners to deliver two previously undocumented Windows RATs, E4del and PINHOLE, using an unconventional technique that helps malicious communications blend into legitimate network activity.

Citrix Urges Admins to Patch New NetScaler Flaws as Soon as Possible | Vulnerability / Network Infrastructure | BleepingComputer

Citrix urged administrators to quickly apply security updates addressing newly disclosed NetScaler vulnerabilities, particularly for internet-facing appliances that could provide attackers with a valuable entry point into enterprise environments.

Rust Supply Chain Attack Puts Build-Time Malware in Crates With 245 Million Downloads | Software Supply Chain | The Hacker News

A compromised maintainer account published malicious versions of three widely used Rust crates that introduced a typo squatted dependency capable of downloading and executing malware during the software compilation process.

GitLab CVE-2026-19478 Comes Under Active Exploitation Within Days of Disclosure | Vulnerability / Active Exploitation | The Hacker News

Attackers began exploiting critical GitLab vulnerability CVE-2026-19478 shortly after disclosure, potentially allowing unauthenticated attackers to modify or delete public projects and manipulate repository data.

Microsoft Entra ID Flaw Rated CVSS 10.0 | Identity Security / Critical Vulnerability | The Hacker News

A critical Microsoft Entra ID vulnerability received the maximum CVSS severity score of 10.0, highlighting the potentially significant consequences of vulnerabilities affecting centralized cloud identity and authentication infrastructure.
