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 September 15, 2026
(Reported on Wednesday September 16, 2026)

Local Government

CISA: Critical VMware RCE flaw now exploited by ransomware gangs | Vulnerability/Ransomware | Bleeping Computer

CISA warns that ransomware operators are now actively exploiting a critical, previously patched VMware vCenter remote code execution vulnerability.

Wyoming Cites LayerZero Security Failures in Switch of State Stable Token to Chainlink CCIP | Vulnerability/Protocol Security Failure | Crowdfund Insider

Wyoming's state-backed stablecoin commission detailed security flaws in LayerZero's cross-chain protocol that prompted a full switch to Chainlink's CCIP.

Financial Institutions

Suspected Black Axe gang leaders face cybercrime charges in the US | Business Email Compromise / Wire Fraud | Bleeping Computer

US prosecutors extradited five alleged leaders of the Black Axe cybercrime network to face wire fraud and money laundering charges tied to global financial scams.

Healthcare

Nationwide Home Health Care Provider Announces Major Data Breach | Data Breach | HIPAA Journal

LHC Group, a US home health care provider, disclosed a major data breach affecting patient information.

Suspected cyber incident disrupts Fenway Health in Boston | Suspected Cyberattack/IT Outage | DysruptionHub

Fenway Health, a Boston healthcare and sexual health clinic, suffered a suspected cyber incident that delayed patient communications and canceled appointments.

Other

CenterPoint Energy confirms customer data stolen in cyberattack | Data Breach | Bleeping Computer

CenterPoint Energy confirmed attackers stole and leaked customer personal data in a breach affecting the US utility provider.

Cisco Secure Email Gateway Flaw Exploited in the Wild, Enables Root Command Execution | Vulnerability | The Hacker News

Cisco warns attackers are actively exploiting a critical flaw in Secure Email Gateway that allows unauthenticated root-level command execution.

Shared Hosting at Risk: LiteSpeed Enterprise Bug Can Grant Root from a Single Tenant | Vulnerability/Privilege Escalation | Security Affairs

A critical LiteSpeed Enterprise flaw lets a single shared-hosting tenant escape sandboxing and gain root on the whole server, prompting a forced patch to version 6.3.7.

Malcious Admin Menu Editor Pro plugin backdoors 1,500 WordPress sites | Supply Chain | Bleeping Computer

Attackers compromised a WordPress plugin developer's site to push malicious updates creating hidden admin accounts on roughly 1,500 sites.

Microsoft Releases Emergency Patch to Fix RDS Vulnerability | Vulnerability | Infosecurity Magazine

Microsoft issued an urgent out-of-cycle security update fixing critical flaws in Remote Desktop Services introduced by the prior Patch Tuesday release.

Threat actors are coming for your AI assets to operationalize their use of AI | Data Breach/Model Theft | CSO Online

Google's threat intelligence group reports state and criminal hackers increasingly stealing AI credentials, models, and source code, plus running distillation attacks to extract LLM capabilities.