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 November 19, 2026
(Reported on Friday November 20, 2026)

Local Government

USDA grapples with security breach as IT staff take multiple systems offline | Data Breach | NextGov

USDA took multiple IT systems offline after its security operations center detected an unauthorized intrusion, with scope and data impact still unknown.

CISA Warns of 4 Exploited Flaws Linked to Ransomware, Cryptomining, and LLMjacking Attacks | Vulnerability | The Hacker News

CISA added actively exploited flaws in Synology DSM, LiteLLM, Apache Axis, and REDCap to its Known Exploited Vulnerabilities catalog, citing ransomware and cryptomining risks.

AI is supercharging vulnerability discovery. What that means for state, local governments amid wave of outages | Vulnerability | StateScoop

Analysts warn AI-driven vulnerability discovery is accelerating software flaws, prompting state and local governments to expect more frequent IT outages.

Financial Institutions

Chase, Visa, Mastercard confirm third-party cyberattacks that may have exposed customers' info | Data Breach | The Register

Chase, Visa, and Mastercard disclosed separate third-party vendor cyberattacks that may have exposed customer payment and personal data.

Healthcare

Hackers steal data of 1.6 million SBC Medical Group customers | Data Breach | Bleeping Computer

SBC Medical Group disclosed two cyber incidents in an SEC filing that exposed personal data of 1.6 million customers and employees.

DotHouse Health Pays $725K to Settle Data Breach Lawsuit | Data Breach | HIPAA Journal

Massachusetts community health center agrees to $725,000 settlement over a 2022 data breach lawsuit affecting patient records.

Other

VMware patches vCenter zero-day exploited in attacks since September | Zero-Day/Authentication Bypass | Bleeping Computer

Broadcom patched a critical VMware vCenter authentication bypass flaw that China-linked hackers have actively exploited as a zero-day since September 2026.

Everything Is a Web Application, Including Your Firewall | Vulnerability/Zero-Day Exploitation | The Hacker News

Attackers actively exploit two unauthenticated PHP code-execution flaws in internet-exposed Palo Alto Networks PAN-OS firewall management interfaces.

A single pull request could have handed attackers the keys to Microsoft's software supply chain | Supply Chain / Vulnerability | CSO Online

Security researchers found a now-patched flaw in Microsoft's WinGet package manager that could have let a malicious pull request steal a maintainer's GitHub access token.

Researcher Demonstrates Database RCE Exploits Affecting PostgreSQL, MySQL and Oracle | Vulnerability/Memory Corruption RCE | The Hacker News

Security researcher reveals proof-of-concept exploits letting low-privilege database users achieve remote code execution via memory-corruption bugs in PostgreSQL, MySQL, ClickHouse, and Oracle.

Nvidia adds possible hack to list of very bad things under investigation | Ransomware/Data Breach | The Register

A ransomware gang claims to have breached Nvidia and threatens to leak stolen data unless a ransom is paid, prompting a company investigation.