

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 Wednesday October 07, 2026
(Reported on Thursday October 08, 2026)**

Local Government

FBI Warns FortiBleed Remains Active After Amassing 86,644 Fortinet Device Credentials | Credential Harvesting/Vulnerability Exploitation | [The Hacker News](#)

FBI and Secret Service warn that attackers continue harvesting Fortinet FortiGate VPN credentials via reused passwords and weak legacy hashing, compromising over 86,000 accounts.

US posts \$10 million reward for accused Chinese 'Hafnium' hacker | Nation-State Hacking/Exploitation | [The Record](#)

US government offers \$10 million bounty for a Chinese national tied to the Hafnium Exchange Server hacking campaign that breached thousands of networks.

Recent Taiwan simulation highlights US cyberdefense gaps against China, experts warn | Nation-State Cyber Campaign / Critical Infrastructure Disruption | [NextGov](#)

Experts cite a Taiwan cyberwar simulation to warn that US cyberdefenses are unprepared for Chinese attacks disrupting civilian infrastructure below the threshold of war.

Other

Hackers exploit critical Atlassian flaw after public PoC release | Vulnerability/Zero-Day Exploitation | [Bleeping Computer](#)

Attackers are actively exploiting an unauthenticated critical flaw in Atlassian Jira, Confluence, and Bitbucket after a proof-of-concept exploit was publicly released.

Unpatched Critical LMCache Flaw Lets Unauthenticated Attackers Run Code Remotely | Vulnerability | [The Hacker News](#)

Researchers disclosed an unpatched critical flaw in LMCache's ZeroMQ-based multiprocess mode allowing unauthenticated remote code execution against LLM caching servers like vLLM.



Hackers hijack Google domains after breaching ccTLD registries | DNS Hijacking / Supply Chain Compromise | [Bleeping Computer](#)

Attackers breached third-party ccTLD registry operators for Ghana, American Samoa, and Sierra Leone to alter DNS records and obtain fraudulent HTTPS certificates for Google domains.

Georgia Power, Alabama Power Data Breach Hits 400,000 Accounts | Data Breach | [Security Week](#)

Southern Company subsidiaries Georgia Power and Alabama Power disclosed a breach exposing account data for roughly 400,000 utility customers.

Encrypted instructions trick Copilot CLI into spilling developer secrets | Prompt Injection / AI Agent Exploit | [CSO Online](#)

Researchers found a prompt-injection technique that hides malicious commands in encrypted text to trick GitHub Copilot CLI into leaking developer secrets.

Eight Malicious npm Packages Downloaded 40,767 Times Deliver Overlord RAT and Stealer | Supply Chain | [The Hacker News](#)

Researchers uncovered eight malicious npm packages tied to a long-running campaign that installed Overlord RAT and info-stealing malware on tens of thousands of downloads.

SonicWall's latest critical flaw indicates a security pattern, not another one-off bug | Vulnerability | [CSO Online](#)

SonicWall disclosed a maximum-severity, pre-authentication SSRF flaw in its SMA1000 appliance, part of a recurring pattern of critical bugs in the vendor's products.

