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 September 10, 2026
(Reported on Friday September 11, 2026)

Local Government

CISA Flags Exploited Cisco, Citrix, Fortinet Flaws, Sets Sept. 12 Federal Patch Deadline | Vulnerability | The Hacker News

CISA added actively exploited vulnerabilities in Cisco, Citrix, and Fortinet products to its KEV catalog, ordering federal agencies to patch by September 12, 2026.

CISA Updates Insider Threat Guide With New Mitigation Advice | Insider Threat | Infosecurity Magazine

CISA revised its insider threat guidance to add mitigation recommendations addressing remote work, AI risks, and detection practices.

Financial Institutions

Gigabud Creates Android Work Profiles to Hide From Banking App Malware Checks | Malware | The Hacker News

Gigabud banking trojan now abuses Android work profiles to hide a fake banking app and evade anti-malware checks on infected devices.

Protecting organizations from AI-assisted executive impersonation and invoice fraud | Social Engineering / BEC | Microsoft Security Blog

Microsoft details an AI-enhanced business email compromise scheme using fake executive emails and invoices to trick finance teams into ACH fraud transfers.

Healthcare

Dental contractor set up secret account with access to 4,000 patient records then left the company | Insider Threat / Unauthorized Access | The Register

A former dental practice contractor created a hidden account granting unauthorized access to roughly 4,000 patients' records after leaving the company.

High Severity Vulnerabilities Identified in NextGen Healthcare Mirth Connect | Vulnerability | HIPAA Journal

Researchers disclosed three high-severity security flaws in NextGen Healthcare's Mirth Connect integration engine used across healthcare systems.

Other

Surfshark VPN says hackers breached internal testing, proxy servers | Data Breach | Bleeping Computer

Surfshark VPN confirmed attackers accessed an internal test server and proxy infrastructure after a misconfiguration left it exposed online.

Check Point Discloses Two 9.8-Rated VPN Certificate Flaws Enabling Unauthenticated RCE | Vulnerability | The Hacker News

Check Point patched two critical, 9.8-severity flaws in VPN certificate handling on its Security Gateways and management software that could allow unauthenticated remote code execution.

Nearly 1 in 10 Exposed LiteLLM Gateways Accepted the Example "sk-1234" Admin Key | Misconfiguration/Default Credentials | The Hacker News

Wiz researchers found nearly 10% of internet-exposed LiteLLM AI gateways still used the vendor's default admin key, risking full data and cost exposure.

AI lets small actors run state-level hacking campaigns, Anthropic report finds | AI-Enabled Cyber Espionage/Malicious Use | CyberScoop

Anthropic report reveals AI models were misused by state-linked and criminal hackers to scale espionage and cybercrime operations, including a Russian-aligned campaign targeting 20+ organizations.