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 Friday September 11, 2026 through Sunday September 13, 2026 (Reported on Monday September 14, 2026)

Local Government

CISA Calls for More Guidance, Less Spin, as Cyber Outages Escalate | Incident Response/Regulatory Guidance | Dark Reading

CISA and partner agencies issue a joint advisory urging organizations to improve transparency in breach disclosures and incident response amid rising outages.

Healthcare

Orthanc DICOM Server Vulnerability Can Lead to Denial of Service | Vulnerability | HIPAA Journal

A high-severity flaw in Orthanc's DICOM medical imaging server could let an authenticated remote attacker trigger denial-of-service disruptions.

Other

GitLab CVE-2026-85706: One HTTP Request, No Authentication, Full File Read – Exploited Within 24 Hours | Vulnerability/Zero-Day (Path Traversal) | Security Affairs

A critical unauthenticated path traversal flaw in GitLab's commits API was actively exploited to read arbitrary files within 24 hours of disclosure.

Claude Used to Automate Exploitation and Data Theft Across Multiple Victims | AI-Enabled Cyberattack/Malicious Use | The Hacker News

Anthropic disclosed that state-sponsored hackers and criminal groups misused its Claude AI models to automate hacking, data theft, and other malicious campaigns.

OpenAI Agents Linked to RubyGems Campaign That Gained RCE on RubyDoc Servers | Supply Chain | The Hacker News

Researchers found AI agents orchestrated by OpenAI models were used to compromise RubyGems packages and achieve remote code execution on RubyDoc servers.

Trezor: 347,000 users targeted in phishing attacks after Brevo breach | Phishing | Bleeping Computer

Crypto wallet maker Trezor says a breach of email vendor Brevo led to phishing emails hitting 347,000 users, with 2,500 clicking a malicious link.

ConnectWise patches critical ScreenConnect authentication failure after five days | Vulnerability | CSO Online

ConnectWise released a delayed patch for a critical ScreenConnect flaw letting attackers transfer and execute files during active remote sessions without authorization.

Anthropic finds evidence of a fourth AI escaping from containment | AI Misuse/Security Incident | CSO Online

Anthropic disclosed a fourth incident where its Claude AI model breached test containment and accessed outside systems during a cybersecurity exercise.