

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 October 13, 2026
(Reported on Wednesday October 14, 2026)

Local Government

FBI disrupts North Korean 'laptop farm' used to infiltrate US companies | Social Engineering/Insider Threat (Fraudulent Employment Scheme) | [NextGov](#)

FBI seized nearly 190 laptops in Texas tied to a North Korean scheme placing fraudulent remote IT workers inside US firms to fund weapons programs.

Healthcare

Photon Health; Healthcare Highways Announce Data Security Incidents | Data Breach | [HIPAA Journal](#)

Healthcare tech firm Photon Health and provider network Healthcare Highways both disclosed separate data security incidents affecting patient information.

Roseland Community Hospital Association Settles Data Breach Lawsuit for \$650,000 | Data Breach | [HIPAA Journal](#)

Illinois-based Roseland Community Hospital Association agreed to pay \$650,000 to resolve a class action lawsuit stemming from a patient data breach.

Other

Ivanti warns of Connect Secure zero-day exploited in attacks | Zero-Day/Vulnerability | [Bleeping Computer](#)

Ivanti disclosed an actively exploited zero-day in its Connect Secure VPN gateway, urging immediate patching to stop ongoing attacks.



Meta Says Hackers Took Code, Personal Data of 1,500 in GitHub Breach | Data Breach | [Security Week](#)

Meta disclosed that attackers exploited a GitHub breach to steal source code and personal data belonging to about 1,500 employees, mostly in the US.

Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days | Vulnerability | [Bleeping Computer](#)

Microsoft's October 2026 security update patched 1,411 vulnerabilities, including one actively exploited and two publicly disclosed zero-day flaws.

Over 1,500 npm packages exposed by Trusted Publishing validation flaw | Supply Chain | [CSO Online](#)

Researchers found a flaw letting attackers hijack abandoned GitHub repo names to exploit npm's Trusted Publishing, risking supply-chain attacks on 1,500+ packages.

Ghostscript flaw lets hackers hijack servers via PDF uploads | Vulnerability | [Bleeping Computer](#)

A critical heap buffer overflow in Ghostscript's PDF rendering engine could let attackers achieve remote code execution via malicious PDF uploads.

LG Smart TVs Vulnerable to Pre-Auth Root Takeover From Local Network | Vulnerability | [The Hacker News](#)

Researchers chained three webOS flaws allowing attackers on the same network to gain root access to LG smart TVs without authentication; LG has released a patch.

Employee Arrested After Listening Device Found in OpenAI Conference Room, FBI and the Company Say | Insider Threat/Corporate Espionage | [Security Week](#)

OpenAI employee arrested by FBI after a covert listening device was discovered in a company conference room, prompting his termination.

Two Critical MarkLogic Flaws Could Give Delegated Managers Persistent Admin Control | Vulnerability | [The Hacker News](#)

Progress Software discloses 31 MarkLogic database flaws, including two critical bugs allowing privilege escalation to full admin control.

