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 January 21, 2026
(Reported on Thursday January 22, 2026)

Government

CISA Adds One Known Exploited Vulnerability to Catalog
Read more at Cisa.gov

Schneider Electric devices using CODESYS Runtime
Read more at Cisa.gov

Financial Institutions

Why Upwind Is Eyeing $250M of Funding at a $1.5B Valuation
Read more at BankInfoSecurity

White House Sees Crypto Bill Inevitable; DCUC Flags Risk Of Credit Card Add-Ons
Read more at CUtoday.info

Healthcare

EHR Vendor Veradigm to Pay $10.5M to Settle Hack Lawsuit
Read more at HealthcareInfoSecurity

OCR Advises HIPAA-Regulated Entities to Take Steps to Harden System Security
Read more TheHIPAAJournal

Other

Zendesk ticket systems hijacked in massive global spam wave
Read more at Bleeping Computer

Cisco fixes Unified Communications RCE zero day exploited in attacks
Read more at Bleeping Computer

Microsoft shares workaround for Outlook freezes after Windows update
Read more at Bleeping Computer

Chainlit AI framework bugs let hackers breach cloud environments
Read more at Bleeping Computer

News from Wednesday January 21, 2026
(Reported on Thursday January 22, 2026)

New Android malware uses AI to click on hidden browser ads
Read more at [Bleeping Computer](#)

Online retailer PcComponentes says data breach claims are fake
Read more at [Bleeping Computer](#)

Fortinet admins report patched FortiGate firewalls getting hacked
Read more at [Bleeping Computer](#)