FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, August 21, 2026

Zoom Vulnerabilities Discovered Using AI Frontier Models

Source: FS-ISAC

On 11 August, researchers from A Security published their discovery of Zoom vulnerabilities (CVE-2026-53413, CVE-2026-53414, and CVE-2026-53415) that could allow attackers to gain remote code execution on another participant's device during a meeting. The flaws impacted multiple operating systems and required little to no user interaction, potentially enabling data theft, credential compromise, malware installation, and surveillance. Researchers also noted that publicly available AI models were able to identify the vulnerabilities and help develop a working exploit in less than 24 hours. Zoom has since released patches and urged users to update affected products.

Financial institutions using Zoom should update Zoom Workplace to version 7.1.5 or 7.0.6 and later, Zoom Rooms to version 7.1.0 or later, Zoom Meeting SDKs to version 7.1.0 or later, and Zoom Workplace VDI Client for Windows to versions 7.0.11 or 6.6.16.

(*Click the heading link to read more.*)

Top News

#StopRansomware: Medusa Ransomware

Source: Cybersecurity & Infrastructure Security Agency

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Department of Health and Human Services (HHS) are releasing this updated joint advisory to disseminate known Medusa ransomware tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as April 2026. Medusa is a ransomware-as-a-service (RaaS) variant first identified in June 2021. Both Medusa developers and affiliates use a double-extortion model where they encrypt victim data and threaten to publicly release exfiltrated data if a ransom is not paid.

The update expands details on Medusa actors' operations, including more specifics about their affiliate model and payment ranges for initial access brokers, as well as a broader list of exploited vulnerabilities. It describes Medusa's opportunistic targeting and use of Interactsh URLs for exploit verification. It also lists additional tools for network enumeration, persistence, and stealth, including detailed PowerShell obfuscation techniques and command-and-control utilities. Additionally, HHS has been added as a co-sealer, providing their insights into Medusa's operations against the Healthcare and Public Health Sector.

- Mitigate known vulnerabilities by ensuring operating systems, software, and firmware are patched and up to date within a risk-informed span of time.
- Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization.
- Filter network traffic by preventing unknown or untrusted origins from accessing remote services on internal systems.

(Click the heading link to read more.)

Fraud's Identity Crisis

Source: Adyen

How verified accounts, familiar behavior and AI are driving fraud in 2026.

Fraud's identity crisis is as much about those trying to catch it as it is about those perpetrating it. While fraud has always been part of commerce, what's changed is where it hides and how it appears.

For most of the past decade, the working model for risk teams was relatively simple: Flag what looks unfamiliar. New devices, unusual locations, credentials that don't match. That logic still holds for what it was designed to catch. But the fraud growing fastest today often doesn't trigger those signals. It comes from verified accounts, recognized devices, behavior that clears every checkpoint.

At Adyen, we process payments across the world's largest commerce environments. What we see in that data is a shift in how risk behaves. It's become automated, iterative, and in many cases indistinguishable from legitimate customer activity until you look across time and context rather than at the transaction in front of you.

Risk teams now face a different type of problem, one where getting the decision wrong has immediate commercial impact. It's a problem that can't be solved by tightening controls alone, especially as it's often the controls themselves that are being exploited.

We need a different approach to decisioning: one that reflects how identity and risk actually behave...

(Click the heading link to read more.)

When ‘Live’ Isn’t Live: Inside the Workflows Undermining Biometric KYC

Source: Q6 Cyber

Biometric KYC has moved from an emerging technology to a mainstream expectation. In Q6 Cyber's recent webinar, 84% of participating financial institution security leaders said they either use biometrics for identity verification or are actively evaluating adoption, while only 16% reported no plans to implement it.

This shift reflects growing confidence in biometric authentication, including facial recognition, voice authentication, and liveness detection, as an important layer in fraud prevention and identity verification. These tools have helped institutions improve security while reducing friction for legitimate customers.

But as adoption grows, so does the challenge. Cybercriminals are increasingly using deepfakes, synthetic identities, and AI-generated personas to bypass traditional biometric controls. Technologies designed to improve the customer experience are also giving fraudsters new ways to mimic legitimate users and defeat outdated verification methods.

As a result, financial institutions must evaluate not only whether they use biometrics, but how effective their controls are against evolving threats. Can your liveness detection identify advanced deepfakes? Are your vendors keeping pace with emerging risks?

These questions were explored during Q6 Cyber's recent webinar. If you missed the live session, the recording is available on demand and offers valuable insights into strengthening identity verification programs against increasingly sophisticated fraud tactics.

(Click the heading link to watch the recording.)

How Financial Institutions Can Help Accountholders Avoid Back-to-School Fraud

Source: SHAZAM

As families prepare for a new school year, fraudsters are preparing, too.

The back-to-school season is full of expenses, deadlines and decisions, creating opportunities for scammers to blend into legitimate activity. While consumers are checking items off a growing to-do list, they are less likely to question whether a request, offer or message is legitimate.

For financial institutions, this presents an opportunity to provide timely fraud education. Understanding how scammers build trust and create urgency can help institutions equip accountholders to recognize warning signs before fraud occurs.

Online shopping scams take advantage of urgency and bargain hunting

Back-to-school shopping often comes with budget pressure. Families want to save money, and students are looking for affordable ways to purchase what they need before classes begin.

Fraudsters exploit that mindset by creating offers that feel too good, or too urgent, to ignore. When shoppers focus on a discount or limited-time promotion, they're less likely to verify who is behind the offer.

These scams work because they feel familiar. The shopping experience appears legitimate until the...

(Click the heading link to read more.)