

August 9, 2026

Popular AI Meeting Notetaker App Lets Anyone Join Any Meeting

This was not on purpose - I hope. The app, TI;dv (too long; didn't view) is a meeting assistant that automatically joins, records and transcribes video calls. It is used by millions including Salesforce, Forbes and others. In late January a researcher discovered a way to access the company's back end and join calls, including government agencies. Generally speaking, AI notetakers represent a risk and when combined with a bug, well, it becomes a problem. I have been part of government meetings - they actively remove AI notetakers from calls. Now I know why. Credit: [Dark Reading](#)

Please check out our blog at <https://www.cybersecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybersecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybersecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

Popular AI Meeting Notetaker App Lets Anyone Join Any Meeting

This was not on purpose - I hope. The app, TI;dv (too long; didn't view) is a meeting assistant that automatically joins, records and transcribes video calls. It is used by millions including Salesforce, Forbes and others. In late January a researcher discovered a way to access the company's back end and join calls, including government agencies. Generally speaking, AI notetakers represent a risk and when combined with a bug, well, it becomes a problem. I have been part of government meetings - they actively remove AI notetakers from calls. Now I know why. Credit: [Dark Reading](#)

Some Baseboard Management Controllers (BMC) Leak Password Hashes

One of the challenges here is that it isn't clear which brand/model/firmware versions are affected. The bottom line is that the BMC, like a Dell DRAC, has an insane amount of permissions and access needs to be secured carefully. BMCs should NEVER be exposed to the open Internet, even though that might be tempting. In fact, they should not even be

exposed to your general internal network - they should be on their own restricted access subnet or VLAN. The problem identified is that some BMC protocols expose password hashes even BEFORE you authenticate, which allows an attacker to do an offline brute force attack on the underlying passwords. As always, if you need assistance, please contact us. Credit: [Security Week](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#). If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at <https://aigip.ai/news/latest-ai-news>

Is OpenAI Astra Really a Breakthrough?

Certainly OpenAI would like you to think it is but other people are not so sure. This includes folks at Anthropic who replicated at least some of what OpenAI is claiming in less than 24 hours, using Fable. What it appears OpenAI did is cherry pick some traditionally hard problems that AI makes less hard and solved them using AI. Is that a breakthrough? OpenAI is hoping its investors think so. Other people say the jury is still out. Credit: [Gary Marcus](#)

Who is Liable if Your AI Goes Off Course?

Let's say you are using an AI - and it doesn't matter whether it is self hosted or an online service - and it makes a mistake? Or even worse, you are OpenAI and it hacks Hugging Face? Who is legally liable? The short answer is you. The long answer is Yooooooooou! Is it possible that you can sue your vendor? Sure, it is possible. Does that get YOU off the hook? Absolutely not. What if your employee uses an unauthorized AI tool and feeds it confidential information? You are still liable. Can you fire that employee? That depends. Definitely want to consult counsel first. Fundamentally, in all cases, the buck stops with you. But we have insurance! Have you read the policy lately? That is a definite maybe. Even if your insurance covers it, you are still liable. BUT, read the post near the end - the law is pretty muddy here, so the legal part could work either for or against you. Either way, you still have to defend yourself. Have questions? Please reach out to us.

Anthropic, Pentagon Clash Over First Amendment Claims

A San Francisco federal judge showed skepticism Thursday over whether the Department of Defense acted lawfully when it blacklisted artificial intelligence firm Anthropic, telling federal attorneys at the onset of a roughly 90 minute hearing that the Pentagon is "at odds with the First Amendment." This is in response to the Pentagon declaring Anthropic a supply chain risk. Anthropic says billions of revenue is at risk while the Pentagon says it must be able to make national security decisions. Attorneys for the government attempted to steer the judge away from first amendment claims. The judge will issue a written ruling - no date. Credit: [AI Today](#)

Meta AI Joins the Club of AI Tool Providers whose AIs Hacked Other Companies

So far none have been sued, YET, but Anthropic, OpenAI and Meta all admit that they hacked other companies without their permission. And even more companies are coming clean. Move fast and break things is the unofficial motto of big tech companies. It is coming home to roost. Credit: [Security Week](#)

Well, AI is Not Perfect

That probably won't surprise many of you. A study by 1Password found that AI failed to properly patch bugs 74 percent of the time. Think about that. Only 1 in 4 AI generated bug patches actually worked according to the study. The researchers took six actual recent bugs in open source software and allowed the AI to generate a patch. The LLMs being tested generated a total of 6,080 patch attempts, which is a reasonable sample size. Worse yet, many times the patches APPEARED to fix the problem, but underneath, they don't. Credit: [ZDNet](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

Is the DoD/DoW Addressing Post Quantum Cryptography?

Yes, the DoD is actively pushing the services to inventory encryption with a requirement to shut down any system that does not support PQC by the end of 2030 (that is too late, but they won't even meet that requirement). The strategy for defense contractors is less well defined but the DoD CIO is calling for changes (i.e. more requirements and more cost) to CMMC to require PQC. SO, no requirement yet, but expect one in the future, so you should start thinking about what you are going to do. Without regard to what DoD does, hackers will soon (next couple of years) have a field day with traditional encryption - which includes every password that you enter into a web screen.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

New York State Adds \$9 Million to the Pot to Help Water Utilities Get More Secure

In light of the attacks against 30 Minnesota water systems and more water systems in at least 6 (or more) additional states, New York is giving grants to 153 water systems to conduct assessments and mitigate findings. In addition, they will provide support from the NY Environmental Facilities Corporation. By the END of next year, the state will have provided nearly \$10 billion to help water systems improve their security. Good for New York. Only 49 more states to go. Credit: [Security Week](#)

Feds Give 3 Days to Path N-able God Mode Flaw Under Active Attack

N-able, is a very popular remote monitoring, management and cyber security software solution. The fact that the feds gave agencies 3 days to patch it, which is virtually impossible in the federal government, tells me that the problem is very serious. If compromised the hackers have full control over the n-central console with administrative permissions. Credit: [The Register](#)

Legislative and Legal Activities

Nothing to report

Education

Small Towns Shouldn't Have to Defend America's Water Supply from Iran

Even though the president doesn't think these attacks came from Iran, the intelligence community from half a dozen countries just sent out a warning that Iran is, in fact, based on the evidence, attacking the water supplies of multiple countries. Jen Easterly, a West Point graduate, Rhodes Scholar, retired Lt. Col with over 20 years in intelligence and cyber operations and former director of CISA wrote an enlightening op-ed in the Times about what is happening to small towns who are being totally overwhelmed by foreign adversaries and the government is not doing enough to help. Read her op-ed [here](#).

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

Cyber Attacks President Blamed on Minnesota Incompetence Extended to Other states

States like George, Michigan and South Dakota, so this is not a red state/blue state thing. While the president says he doesn't think it was Iran, other experts like the Water ISAC disagree. I am sure we will find out more over time, but in the meantime Cities from the east coast west have been under attack. It is likely that the attackers are still checking things out including response scenarios, so do not assume this is the end. Credit" [Security Week](#)

Brinks Home Security Hacked

4.9 million records were stolen from their Salesforce instance, a common attack vector for the hacking group ShinyHunters. The good news is that they don't use Salesforce for home security, so this is a pretty vanilla attack; the usual kind of data was stolen and the usual process. Still, it is embarrassing for them. Credit: [Security Week](#)

Crypto Hardware Wallet Flaw Drains \$89 Mil Across Thousands of Wallets

The (supposedly) most secure way to store crypto is in a hardware wallet which is not connected to the Internet. It appears that this is related to a firmware bug in the COLDCARD hardware wallet. 1,082 Bitcoin was removed from 1,196 addresses within 41 minutes. Two later attacks brought the number of addresses drained to 4,585. The error was introduced into the firmware in 2021, so it has been there for 5 years. Upgrading the firmware does not eliminate the vulnerability of existing keys, unfortunately. The only way to truly fix it is to create a new wallet and transfer all of your money to the new wallet, which is inherently scary. Credit: [Hackread](#)

CAF Bank Back Online - Offers Charities \$10 for Their Pain

I am completely serious. They said as a result of the 10-day-long outage they are graciously offering customers to waive the monthly service fee of 5 Pounds. They also said that the service could go down again at any time, but they will try to make that happen over a weekend. Any charity that stays with this bank is crazy. Credit: [The Register](#)

Abbott Laboratories Lost 30 Million Records From its Cancer Diagnostics Biz

Abbott lost 30 million rows of customer data including over a million socials to Shinyhunters. Data includes names, emails, phone numbers, physical addresses, dates of birth and some socials. Credit: [My Privacy Blog](#)

AI Can Switch DNA Results in Software Used by Many (Most?) Major Forensics Labs

Here in Colorado we have an ongoing court case where a longtime government forensic scientist is causing the reopening of hundreds of cases, even though she claimed that she never changed results. One lab; hundreds or thousands of cases. What if nationally, the chain of evidence of DNA could not be assured. How many cases would that impact? It's real. Details [here](#).

DHS Surveillance Growing Dramatically

From DHS viewpoint, they are looking for lawbreakers. But in order to do that, they are perfectly willing to eliminate what little privacy people have left. And, oh yeah, the GAO said that DHS failed all six core privacy protections. Learn more [here](#).

When AI Screws Up, Who is Liable?

When a driverless car crashes and kills someone, who is charged with vehicular homicide? When Meta's or OpenAI's or Anthropic's LLMs hack some company, who committed the crime? The short answer is that this is uncharted territory and the laws don't really effectively apply. But that doesn't mean you won't get sued. Learn more [here](#).

Security News for the week ending August 7, 2026

This week's news: Data center approvals in Texas halted, DEFCON security conference is latest to ban smart glasses with recording, in case you thought Flock surveillance is okay, cyber attacks on water utilities now hit more than a dozen states and if some legislators have their way, get ready for radical changes to the Internet. Details [here](#).

Critical infrastructure is truly in the attackers' crosshairs. The government may not consider you critical but with AI, hackers can attempt to break into a lot more sites. The AIs work 24x7 without vacation. Is your company up to the challenge? Would you detect a subtle hack? If you are not sure, we can conduct an assessment and give you feedback on your security posture. Contact us for details.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663