

August 23, 2026

ChatGPT Updates Apple Messages Integration

This update adds a new Mac integration. It will allow OpenAI to access your iMessage, SMS and RCS messages in order to read received messages and send outbound messages. In case you don't trust giving OpenAI full access to read your messages, that is probably smart. Use at your own risk. Credit: [9to5 Mac](#)

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

Nothing to report

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>

Co-Pilot Snitch Allows Hackers to Steal AI Data Using Undocumented URL Parameter

Varonis Threat Labs has disclosed three vulnerabilities in Microsoft Copilot Personal that it said could allow a single click on a crafted link to silently pull data from connected apps and other information available to the victim's Copilot session. This was disclosed in December and patched this month, but now that it is out there, it will likely be exploited in the wild quickly. Credit: [The Hacker News](#)

Hackers Have New (Expensive) Denial of Service Attack Method

When OpenAI attacked Hugging Face, Hugging Face had to spin up a new AI capability to identify and defend against the attack. This AI used a LOT of tokens. Unless you have a fully operational internal open weights model based AI cluster in your “basement”, you are going to need a cloud based AI to do that and that AI will use a bunch of tokens. Even if the hackers don’t get in, the defense might cost you tens of thousands of dollars in tokens. Ponder that for a minute - a new FINANCIAL denial of service attack because that money takes the money away from something else.

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.

DoD Tells 30 Research Institutions to Review Their Foreign Ties and Report in 2 Weeks

DoD issued a formal notice for these research centers to do a comprehensive review of their financial, academic and research ties to “foreign entities of concern” (aka China mostly). This is designed to protect the DoD from unauthorized technology transfer to foreign governments. And, oh yeah, you have two weeks to do that. Are DoD contractors next? Credit: [DoD](#)

Watch out for this landmine in year three

One of the things that happens when you go for reassessment after three years is that the assessor will ask you to produce the documentation that, for example, you annually reviewed the effectiveness of the security controls in place. Short version - if you can’t produce that you fail and you have to start over with a new assessment. That is likely something that cannot be put on a PoAM because you can’t fix the past.

NEW SPRS/PIEE System Access Requirements

This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

Training Escorts

If you have people like, say, an air conditioning vendor or a furniture repair person (or computer maintenance) and that person does not have a lawful purpose to access CUI, that person likely has to be escorted. But what is your training for that escort? They need to understand what they need to look out for and alarm on. If you need help with this, please contact us.

Reference

Colorado Releases Proposed Rules for AI-Assisted Hiring and Employment Decisions

The first question is whether what you are doing is covered by the law. Being ignorant of the law is not a defense. You are likely required to disclose a lot more information than you historically have been. Learn more from [Fisher Phillips \(law firm\)](#).

Software and Hardware to Check Out

ChatGPT Updates Apple Messages Integration

This update adds a new Mac integration. It will allow OpenAI to access your iMessage, SMS and RCS messages in order to read received messages and send outbound messages. In case you don't trust giving OpenAI full access to read your messages, that is probably smart. Use at your own risk. Credit: [9to5 Mac](#)

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

United Health Sued for Ignoring Cybersecurity, Leading to Massive Breach

Two groups of investors are suing UnitedHealth, alleging they defrauded Medicare, manipulated earnings and ***ignored cybersecurity gaps for years***. They say United rushed the acquisition of Change Healthcare, leading to cybersecurity gaps that resulted in the largest healthcare breach in US history. They say the company and several current and former executives and board members are responsible for ***“corporate governance failures on a historic scale”***.

Credit: [Healthcare Dive](#)

DoJ Settles Child Privacy Litigation with TikTok/ByteDance for \$400 Million

TikTok settled with the DoJ over their lack of compliance with the Children's Online Privacy Protection Act. They will pay \$300 million to start (or roughly 0.2% of one years' revenue) and another \$100 million later. They did not admit any wrongdoing and agreed to implement a few additional controls to protect kids. Basically, a one-time get out of jail free card for what amounts to a rounding error on their books. DoJ of course is pushing this as an amazing win. Which it is not. But it is one more chink in the armor of big tech. Details at [DoJ](#).

Education

Score One for the Defenders

North Korea has a long history of cyber attacking. And, they are good at it. Now (at Blackhat) a security researcher is detailing, to some extent, what he discovered after he hacked the hackers. He had access to North Korea's hacking underground - including servers, Slack, Discord, etc. He documented intrusions, in some cases really damaging intrusions, into over 1,600 companies. Some of which have been confirmed by Japan's CERT. In at least some of the cases, it was third parties that had access to company resources. As these names are becoming public the companies are putting their spin doctors into overdrive (it wasn't us, it was a vendor/contractor that we hired and didn't manage effectively, so you shouldn't blame us for our lack of oversight, right?). Gives you some insight into ***what you don't know you don't know***. It should also give you a healthy dose of are we doing enough monitoring. Credit:

[Wired](#)

Bloomberg on the Meta Trial and Potential \$1.4 Trillion in Damages

For years big tech has dodged responsibility for what some people say is serious harms, especially to young people, that their platforms cause. This trial is one of several and it is brought by 29 state AGs who claim not that the content is harmful but that the algorithms are harmful and Meta has not gotten the charges dismissed. We don't know if they will settle - that often happens after the jury is selected - but what is at stake here is existential to Meta. \$1.4 trillion is basically the entirety of Meta's market capitalization and what the AGs want is for Meta (and others) to change their algorithms, which is the sauce that allows them to capture

incredibly valuable user data. This reporter, from Bloomberg Tech, did a great job of explaining it and I RARELY say that about reporters. [Video 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.

Ring Central Gets its Bell Rung

1.6 million RingCentral users got their information hacked - names, physical addresses and phone numbers. The attack was sophisticated, they say, because, I presume, they would not have fallen for an unsophisticated one. Social engineering, courtesy of ShinyHunters. They claim to have taken 600+ gigabytes of data, which means there was a lot more than a million names and phone numbers. Credit: [The Register](#)

UT San Antonio Takes Systems Offline After Attack

UT San Antonio serves 40,000 students across 6 campuses and had to take some systems offline over the weekend. This includes phones! This forced them to extend the deadline to pay the university as the fall semester started and changes were made to other systems as well. They told everyone to change their passwords, but of course, if 40,000 people try to do that at once, things did not go as planned. *UTSA is also the home of Texas Cyber Command.* Credit: [The Record](#)

Lender Heights Finance Loses Data on 750,000 Customers

Height runs debt consolidation lending companies in multiple states under many brands. Data stolen includes sensitive financial information as you might expect from a lender. They have more than 285 offices across the country. Credit: [The Record](#)

Where the World's Social Media Age Bans Actually Stand

Kids and social media don't necessarily mix well. So lawyers around the world are trying to figure out how they would solve it. Of course, kids are way smarter than old lawyers, but that doesn't stop these guys from trying. [Here](#) is where the laws stand.

Feds Allow Private Companies to Hack Hackers

It will be interesting to see how effective this is and what the hackers' responses will be. If one of these government vendors successfully hacks a hacker, what is the hacker's response? It could be nuclear, like, for example, poisoning the water supply in some town not related to the original hack. Or, maybe, destroying all of the data and backups of say, a hospital. It could get dicey. But the government is doing it, so stay tuned. Learn more [here](#).

White House Making 180 Degree Turn on AI Regulation

After running on a platform of absolutely zero regulation on AI vendors, the president has issued a classified order that would ask AI companies to "voluntarily" submit their models to the NSA for "review" before release. You saw what happened when Anthropic declined that request, so voluntary needs to have an asterisk next to it. Learn more [here](#).

Security News for the week ending August 21, 2026

This week's news: Catch and release, cybersecurity edition, OpenAI institutes new safeguards, you see a hot chick-you don't look them up in the [Flock] database, Anthropic plans to watermark Claude's AI-generated text and FCC bans foreign made robots and connected power inverters. Learn more [here](#).

Colorado has released rules for disclosing your use of AI. If you are or plan to use AI to automate your business processes you need to understand what the law requires of you. While Colorado's law is the first, others will follow suit. Contact us for assistance.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663