

Apr 26, 2026

Florida AG Opens Criminal Investigation into ChatGPT

People use AI for all sorts of things. What we are discovering is that the "go-to" defense that companies who write and use software use to wiggle out of lawsuits most of the time is probably not going to work this time. That means that companies that write and use AI software need to pay attention to what the courts say in the many cases that have already been filed and will be filed in the future to help them manage the risk. Learn more [here](#)

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

China Announces Global 24/7 Satellite Reconnaissance Coverage Including US Navy

China claims that these satellites - just 3 of them - flying at 25,000 miles above the earth and therefore effectively, impossible for us to disable or blind, gives them real-time reconnaissance of the entire ocean, which, of course, includes all US Navy assets. In this case, they made a point to let us know that they are watching. Likely we can do the same, but we would prefer it if we had the advantage. Credit: [Tech Radar](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

Anthropic Won't Own Design Flaw in MCP

MCP or Model Context Protocol, a very popular technology that allows AI tools to integrate with the rest of the world, has a design flaw that allows hackers to take over hundreds of thousands of MCP servers that are publicly visible. Anthropic's solution, like software vendors often do, was to choose between fixing the problem and fixing the manual. They chose to fix the manual

because changing the protocol would likely break some applications that use it. SO, BEWARE, if you use MCP, there are issues with the security of it. Credit: [The Register](#)

Florida AG Opens Criminal Investigation into ChatGPT

People use AI for all sorts of things. What we are discovering is that the "go-to" defense that companies who write and use software use to wiggle out of lawsuits most of the time is probably not going to work this time. That means that companies that write and use AI software need to pay attention to what the courts say in the many cases that have already been filed and will be filed in the future to help them manage the risk. Learn more [here](#)

Anthropic Mythos in the Wild

A Discord-linked group accessed Anthropic's Mythos according to Bloomberg. The breach may have been linked to a third party contractor who had their shared accounts AND API keys used by unauthorized users. The group, apparently, was only interested in learning about the model and not using it to hack others. Anthropic is investigating. Credit: [Hackread](#)

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.

Q: What is the latest information from L3Harris about what their subs need to do

A: L3Harris sent out a memo (see <https://tcps-blog.com/cmmc-reqs>) that says all suppliers who receive CUI need to be certified as required in the contract. This is pretty typical. What is not typical is that they are asking for a copy of your C3PAO (third party) certification letter and a copy of the final report from the C3PAO. And, they want it no later than July 30th. This is literally impossible if you have not started yet. While this is the most aggressive requirement we have seen so far, it will likely be the norm as the primes protect themselves from being hit with False Claims Act lawsuits themselves.

Reference

Claude Mythos bug hunting era has begun

Mythos found 271 bugs in Firefox. That is just a start. It is not that these bugs could not have been found by a human, it is just that they were not. A previous version of Claude's software found 22 bugs. This version found more than ten times that many bugs. For companies that don't use Mythos and similar tools to hunt for bugs in their software, they are, long term, in a world of trouble. Credit: [CSO Online](#)

Software and Hardware to Check Out

Google Unveils Agentic AI Data Cloud

It is not really a new product, but it is existing tools packaged together to support the writing, deployment and management of AI agents. It includes a "knowledge catalog" and a cross-cloud (AWS, Azure and Google) data lakehouse and a data agent kit. The formal name for it is the Agentic Data Cloud. These kinds of capabilities are going to be a requirement for companies writing agents at scale. I am sure that Amazon and Microsoft will release similar capabilities soon. Credit: [Tech Target](#)

Important Issues/Patches

Vercel Breach - Third Party Breach with a Fourth Party Cause

Vercel is a cloud platform and AI cloud for developers and created and maintains the [Next.js](#) framework used by companies like Nike, Uber and others. It is the fourth most used web framework. They were hacked and some of their customers' data stolen. They are telling affected customers to rotate credentials. They say that hackers compromised a third party tool (third party to them, fourth party to you) Google Workspace account and were then able to get access to certain environment variables which were not marked as sensitive, so not encrypted. This is a textbook story (see details at link) of the attack chain that shows that the attack chain is long and you have to protect it all. Credit and details: [Computing](#)

Legislative and Legal Activities

Alabama passes privacy law with some twists

Alabama passed its law unanimously in both houses, which by itself is amazing. It has one of the lowest data thresholds in the country and a middle of the road definition of data sale. It exempts businesses with less than 500 employees but only exempts non-profit organizations with fewer than 100 employees and then, only if they don't sell data. There are a number of other twists, so businesses with visitors or customers from Alabama should take note. Credit: [Ballard Spahr \(law firm\)](#)

Education

Nothing to report

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.**

Aave Lending Protocol Faces \$200 Mil in Bad Debt After Exploit

Aave is a "DeFi" or Distributed Finance Lending Protocol that uses Cryptocurrency and the Block Chain to create a community of lenders and borrowers outside of the normal banking channels with no recourse if something goes wrong. Which it too often does. In this case to the tune of between \$117 and \$236 million. They have a rainy day fund of \$50 million, which leaves someone holding the bag. Not the hackers. And this is before hackers have the ability to forge blocks on the blockchain using quantum computing. Credit: [Web 3 Is Going Great](#)

Rutan & Tucker Law Firm Breached

This is a relatively small law firm, generating around \$64 million in revenue and headquartered in California, so normally, it would not make this list, but given they stole case files and other confidential information, this is a BIG problem for the firm. Credit: [Daily Dark Web](#)

Shocker! Federal ban on Anthropic is for show

While Anthropic is tiny compared to OpenAI in terms of users, it actually generates more revenue. Now the feds are trying to make multiple deals with Anthropic even though Secretary Hegseth says they are a supply chain risk. Treasury, Commerce and even the White House disagree. Details [here](#).

5 API calls exposes every Lovable project built before last November

Lovable is a low code/no code software development tool and how they handled this bug is a case study on how NOT to handle situations like this. All it takes is a free account plus five API calls to steal data and credentials and even full source code. The problem is that when you allow non-developers to develop code, it is likely they are not going to know how to develop secure code. Details [here](#).

Indian medical student is fake MAGA influencer

Seeing is not believing. This guy made more money every month selling swag and porn to MAGA types pretending to be a pro-Christian, pro-second amendment and pro-life young nurse than he could as a professional in India. While this is targeted to MAGA supporters, others are not immune, so look at what you see with a critical eye. Details [here](#).

Security News for the week ending April 24, 2026

This week's news: man sues Reno over facial recognition that got him wrongfully arrested, well, this may not work out right, CISA director saga continues, nomination withdrawn, FCC expands ban on foreign routers and largest hacking network shows 10x growth in a year. Details [here](#).

Are you using AI to hunt for bugs in software that you use internally or sell? If not, you are giving hackers a definite leg up. Need assistance with figuring out how to use this fast moving toolset? Contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663