

August 2, 2026

Chinese Release Model Weights, Tech Information on Kimi K3

The Chinese would like nothing more than to throw a giant monkey wrench into the US AI industry. They are doing pretty good at it right now. They have released the model weights, tech report and tech blog for Kimi K3. This is all that someone with enough compute to run the model, which might be \$100k to \$500k+ in hardware, to run a model which is not quite as good as Mythos, but close (and a lot slower). Still, it is free, taking out the cost of the hardware, and a lot of people are considering it. [Here](#) are the links to the downloads.

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

Google Patched More Than 1,000 Chrome bugs in the Last Two Releases

AI to the rescue. Google said that in the two June releases of Chrome, they patched 1,072 bugs. In the previous TWO YEARS they patched 1,036 Chrome bugs. If you are a defender, what changes are you making to protect yourself? Credit: [Tech Crunch](#)

Hacking Group Threatens EU if they Don't Abandon Chat Control Plans

Chat Control is the EU plan/requirement to have phone makers scan all of the content on your phone for things the EU doesn't like. Right now this includes child porn, which very few people are in favor of, so politicians thought this was a safe way to start surveillance of peoples' phones. The hacktivist group LunarisSec says that they have discovered vulnerabilities in EU systems and are threatening to exploit them unless the EU abandons Chat Control. It seems highly unlikely that the EU would agree to this, so now we are waiting to see what the hackers will do. Assuming they are sophisticated and have access to locally hosted frontier AI tools like Kimi K3 or Z from China, their threats could be completely valid. Uh, Oh! Credit: [Cybernews](#)

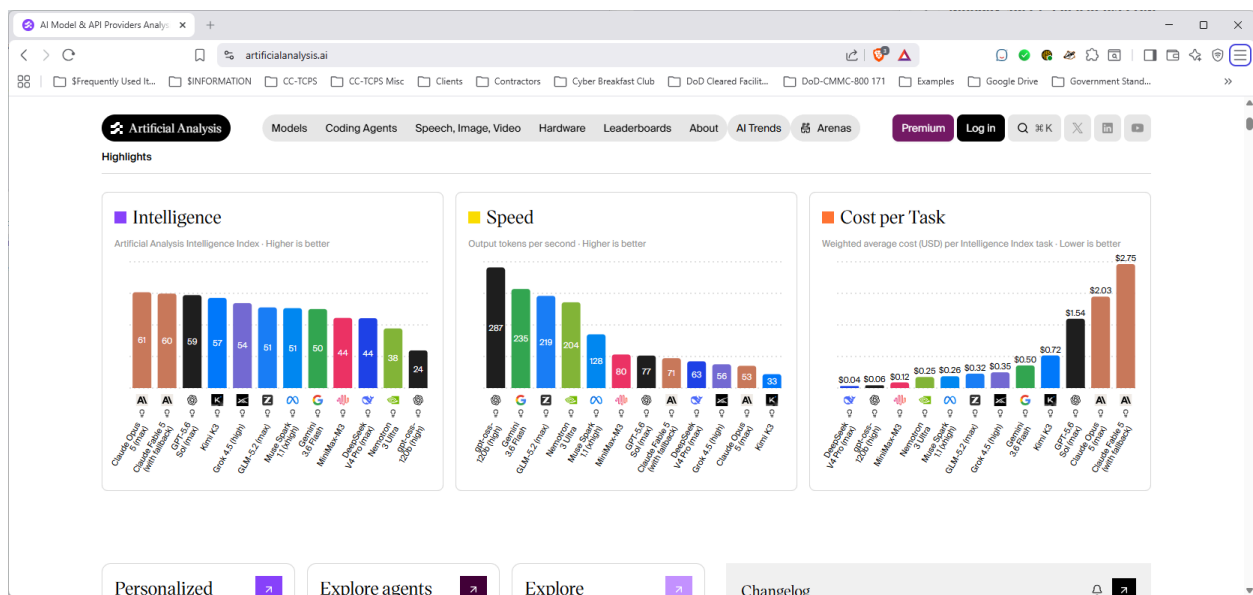
AI Alerts

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>

Which AI Should I Use?

As companies are experimenting with AI, they don't have a strategy for which AI to use. I think, ultimately, it is going to come down to cost. Now is the time to start thinking about that and, at least at the beginning, it is not going to be simple to figure out. Check out this chart from [ArtificialAnalysis.ai](https://www.artificialanalysis.ai)



It is a bit of an eye chart here but go to the web site. They are comparing how intelligent a particular AI is, how fast it is and how much it is going to cost to complete a task. If you need assistance with this, please contact us.

Microsoft Unveils MAI-Cyber-1-Flash - Cybersecurity AI at Half the Cost

The model is built into Microsoft's internal AI security tool MDASH. They claim it reduces security AI costs by 50% and handles 90 percent of routine tasks. A public preview will be available November 3rd.

Impact of OpenAI's Hack of Hugging Face

Now that OpenAI has officially admitted that they are responsible for hacking Hugging Face, we are seeing an amazing chain of events from a bill in Congress to allow the government to kill an AI to Europe saying they need their own AI because they don't trust us. Check out the details at <https://tcps-blog.com/the-fallout-from-the-hugging-face-attack/>

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.

Nothing to report this week - maybe

People are waiting for the DoD's plans for CMMC going forward, but it looks highly unlikely that they will cancel it. What looks more likely is that they will speed up the requirement for NIST SP 800-171 Rev 3 to align with the release of the FAR CUI rule either late this year or early next year. Waiting is not a great strategy.

Reference

Chinese Release Model Weights, Tech Information on Kimi K3

The Chinese would like nothing more than to throw a giant monkey wrench into the US AI industry. They are doing pretty good at it right now. They have released the model weights, tech report and tech blog on K3. This is all that someone with enough compute to run the model, which might be \$100k to \$500k+ in hardware, to run a model which is not quite as good as Mythos, but close (and a lot slower). Still, it is free, taking out the cost of the hardware, and a lot of people are considering it. [Here](#) are the links to the downloads.

Software and Hardware to Check Out

Google is Working on Yet Another New AI Chip

Every week we have a new player in the AI chip biz. Of course, Google is already in that business with their current AI chips which they call Tensor Processing Units. Version 8 was announced in April and is not even available yet, but they are already working on something code named Frozen v2. It is a server AI chip. Credit: [Tech Crunch](#)

Important Issues/Patches

Nothing to report

Other than, that is 622 Microsoft patches, 1,449 Oracle patches, over 1,000 Google Chrome patches. Do you see a trend here?

Legislative and Legal Activities

New York Court Ruling Significant for Tech Firms

The CFPB, before it was pretty much neutered by the president, was going after Zelle (AKA Early Warning Services) for not preventing fraud on the platform. I am not sure what the logic was in the legal name of Zelle (early warning), but one might think that it should provide an early warning to its customers. After the CFPB dropped the suit, the New York AG took basically the same evidence and filed suit under New York state law. Zelle tried to get the case dismissed under the theory of "we're just a platform, we are not responsible for what happens on the platform". That worked for the likes of Facebook and Twitter for years, but lately judges are much less sympathetic. Same here. This case is only at the procedural stage, but the judge denied most of the theories that Zelle came up with and the case will likely go to trial, unless Zelle figures that a verdict against them would be problematic and tries to settle out of court. 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.**

South Carolina/Georgia Health System Closes Offices After Malware Attack

AnMed, a non-profit health system serving South Carolina and Georgia had to shut down dozens of departments due to a malware attack. Urgent care services are open but imaging, Obgyn, primary care and medical groups (doctors) are all closed. They run 4 hospitals and 60 doctor practices. Credit: [The Record](#)

UK-Based CAF Bank Down for a Week; 14,000 Customers Have No Access to Money

CAF bank suspended online banking a week ago and does not even have a timeframe for restoring access to 14,000 charity customers. The bank detected a vulnerability, previously unknown, between the bank and a third party vendor the bank uses. Core banking services, they say, are okay, but customers can't get to them. CAF is basically an online-only bank, so customers can't visit a branch to get their money, assuming that is even possible. The bank has about \$2 billion in deposits. MPs in parliament are saying that the UK's charity regulator, the **Charity Commission** "does not appear at all fit for purpose" to handle sector wide crises.

Credit: [The Register](#)

Nvidia and 36 friends form Open Secure AI Alliance

Nvidia and 36 friends like Microsoft and Cisco have formed this alliance to share tools and information for defenders to use to protect themselves from Alliance members' products being used by bad actors. While this may help some defenders, they hope it also will help their public image. Still, check it out. Details [here](#).

Meta is facing \$1.4 trillion in liability over social media addiction

Even for Meta, \$1.4 trillion is a lot of money. Meta's market capitalization is only \$1.5 trillion. They are facing lawsuits across the country and likely they are going to try to settle the suits quietly, without creating any precedent. We shall see if they are successful. Details [here](#).

The fallout from the Hugging Face attack

Details of the Hugging Face attack are becoming public. The victims and the offenders both, are coming clean and it is useful for defenders. If you think that just because you are not using AI you are safe, you are not. If you need assistance, please reach out to us. Details [here](#).

Security News for the week ending July 31, 2026

This week's news: Even Angelia Jolie and Robert DeNiro get hacked, post quantum cryptography vs Mythos, what is the weak spot in the electricity grid worldwide, US Space Force has new way to jam enemy satellites and data center builders are testing a new strategy to get enough water. Details [here](#).

Are You Prepared for an Incident Like the One at CAF Bank (Above) Currently Unfolding?

While this incident is in the UK, there is no reason to think the US banking system is immune to this. Your business continuity plan needs to consider an event like this. It seems like these organizations don't even have basic financial knowledge, never mind advanced knowledge. I am sure that you can see several obvious solutions here. If you need assistance, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663