

August 16, 2026

A Tiny Little Security Misconfiguration

A YouTube video calls out OpenAI and Anthropic for trying to out-do each other with “our security breach is bigger than your security breach”. I have no idea who this lady is but she is not pulling any punches and tends to use some words that are better off at home than the office, if you get my drift. Still, she nails both companies. Just nails them. It would be funny if it (a) wasn't true, (b) didn't indicate that Silicon Valley does not have their act together when it comes to AI and (c) didn't smell like a ploy to jack up the price of their IPOs. Definitely entertaining. And she makes some really interesting points starting at about the 12 minute mark. Available for the moment on [YouTube](#).

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

Flock Planned to Turn 350,000 Uber, Lyft and Delivery Drives into Surveillance Sources

A leaked pitch shows they planned to add 350,000 rideshare and delivery cars to its license plate reader network. They were or are going to use Nexar dashcams, but a deal has not happened yet. Needless to say, this raises a lot of privacy concerns. They currently have about 180,000 cameras, so this would triple the number of cameras they have. Credit: [Cybernews](#)

Cities Are Ditching Flock. Why? To Be More Covert

As citizens get more upset about Flock and have resorted to destroying Flock cameras, some cities are moving to Axon. Is this because Axon doesn't have as bad a reputation yet? Maybe. But also because Axon cameras can be mounted on existing street lights making them less visible and harder to attack.



Image: screenshot from Axon YouTube video

Unlike Flock, Axon does not have a national database of all of its data, which inherently makes it a bit more privacy focused. On the other hand, their lamp post cameras can livestream. Pick your poison. Credit: [404 Media](#)

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>

A Tiny Little Security Misconfiguration

A YouTube video calls out OpenAI and Anthropic for trying to out-do each other with “our security breach is bigger than your security breach”. I have no idea who this lady is but she is not pulling any punches and tends to use some words that are better off at home than the office, if you get my drift. Still, she nails both companies. Just nails them. It would be funny if it (a) wasn’t true, (b) didn’t indicate that Silicon Valley does not have their act together when it comes to AI and (c) didn’t smell like a ploy to jack up the price of their IPOs. Definitely entertaining. And she makes some really interesting points starting at about the 12 minute mark. Available for the moment on [YouTube](#).

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.

What is DoD Doing under the CMMC Review?

The hope was that DoD was going to simplify CMMC, but if you listen to the DoD CIO, it seems like she wants to add new requirements like post quantum encryption (not currently in 800-171) and phishing resistant MFA (nope, not there either). In fact, it seems like she is saying that 800-171 DOESN'T go far enough. We don't know, of course, but we don't see any indications that they are going to simplify anything. Stay tuned.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

N-able Releases Second Hotfix as Attacks Continue

For users who installed the first N-able patch as N-able systems were under attack, N-able had to release a second patch. N-able says that hotfix 2 is required even if you already installed hotfix 1. They call it "expanding protections". I call it a band-Aid on top of a Band-Aid. I am not familiar with the details of the first fix, but it is often the case that a vendor patches the symptom and not the root cause. Since the company calls the new attack a "variant", it would appear that is just what they did. If you use N-able, time to patch. Again. Credit: [Help Net Security](#)

Microsoft is Improving - Only 400 Patches This Month

While 398 patches this month is better than 622 patches last month, I don't think we should be celebrating. Let's see what happens in the next 6-12 months. In the meantime, get to patching, again. Can you imagine that we would be saying that in June they patched ONLY 200 bugs? Credit: [Brian Krebs](#)

Legislative and Legal Activities

Colorado Publishes Draft ADMT Regs

Colorado's landmark AI law (SB 24-205) is now in the dumpster and replaced with a very lightweight version of its former self. SB 26-189 will go into effect on January 1, 2027 and is limited to AI systems that are high risk and may cause algorithmic discrimination that processes personal data to materially influence a consequential decision. If it does then you have to tell people you are doing that, explain any adverse decisions and give people the opportunity to correct any bad data that you used. People can no longer sue. Basically, pretty meaningless, which is exactly what the industry wanted. Credit and details at [Ballard Spahr \(Law firm\)](#)

Education

Google's Post Quantum Crypto (PQC) Strategy 101

I have written several pieces on PQC lately. It is going to become more important as we get closer to Q-Day, the day quantum makes traditional encryption useless and all encrypted data that was stored becomes plain, unencrypted text. They have really done a great job here and it is laid out in detail. Hopefully, your other vendors (AND YOU) have a similar strategy. Find the strategy [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.**

Shipping Giant Ceva Logistics Breach Impacts Banks, Retailers and Others

France based Ceva has over a thousand warehouses worldwide. Even if we have never heard of them. They brought in close to \$20 billion in revenue last year. Now a cyberattack is causing shipping delays. They are often targets so that hackers can sell the data of where trucks are and what they hold to crooks that hijack them. Credit: [Tech Crunch](#)

Hacking Group ExfilSquad Launches Stolen Data Web Site

This group focuses on stealing data. Recent thefts include UK police officers, UK Department of Education, the cities of Atlanta and Houston. Within one day they announced the hack of 15 organizations. For organizations that did not pay, the data has been posted publicly, a bell that cannot be unrung and the start of a raft of lawsuits for those companies. Frontier Airlines is also among the companies compromised. For Frontier, they were notified by an ethical hacker in March that its mobile API and website were exposing data. The airline fixed most but not all of the bugs by June, three months later. Apparently, ExfilSquad got there first. Credit: [Data Breach Today](#)

Another Microsoft Defender Zero Day - ShieldBreak

The researcher who calls himself or herself Nightmare Eclipse continues to be a nightmare for Microsoft, releasing another zero day ON patch Tuesday along with a proof of concept. I keep saying it is in Microsoft's best interest to make peace with this person, but no, they won't. The researcher says that the new vulnerability gives you full SYSTEM permissions on a fully patched Windows 10,11 and Server systems. The proof of concept was tested and had a 100% success rate. Take that Microsoft. Hopefully Microsoft will rethink its strategy. Otherwise, expect a new zero-day every patch Tuesday. Credit: [Bleeping Computer](#)

Open weight LLMs are NOT open source software

Meta released a new open weight LLM last week called Meta Glimmer. The New York Times reported that as open source software, which PBS repeated. It is not. Not even close. And, it is not only open weight, but light weight. Learn more [here](#).

I'm from AI and I am here to help you

Microsoft patched 400 bugs this month and 600 last month. Researchers let AI agents loose on the software that runs our 4G and 5G cell networks and they found 84 security vulnerabilities nobody had found before. Samsung patched 176 vulnerabilities in their phone apps. Zoom has a ZERO CLICK REMOTE CODE EXECUTION bug that allows a hacker to compromise meeting participants. That is only the start. Thanks AI. Details [here](#).

The blockchain is supposed to be immutable - until it is not

Blockchain's claim to fame is that it can't be changed. Well, that is not quite true. Two incidents were reported last week, both of which involved changing the unchangeable blockchain. Details [here](#).

Security News for the week ending August 14, 2026

This week's news: Apple's chip maker is sitting on a billion dollars of chips waiting for memory, bet you didn't think of this captain obvious, more law enforcement personnel arrested for stalking using Flock cameras, FBI agent accused of stealing \$1 million in crypto and cops are being told "DO NOT MENTION AUTOMATED LICENSE PLATE READERS". Details [here](#).

As AI vendors like OpenAI admit that they were (or are) clueless about how to secure their networks in the age of AI, others are saying it is far from impossible. What is impossible is to hope that you will magically be protected if you don't take the right actions. If you need assistance, contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663