

Mar 8, 2026

AWS Has a Bad Day

AWS said that “external objects”, AKA missiles or drones, struck an AWS data center, ME-CENTRAL-1, and caused significant damage - see photo below. They also said that events like this where entire data centers or regions go off line - that is your problem, not theirs. Learn more below.

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

AWS Has a Bad Day

AWS said that “external objects”, AKA missiles or drones, struck an AWS data center, ME-CENTRAL-1, and caused significant damage - see photo below.



AWS confirmed that “availability zone” mec1-az2 was hit and that the fire department cut all power to the site, including UPSes and generators, to fight the fire. As a result THREE availability zones in the middle east are either down or severely degraded. This was on Sunday. On Monday, availability zone mec1-az3 went offline and AWS changed the area’s status from degraded to disrupted. AWS Bahrain is also showing failures and degraded responses.

AWS is telling customers of those data centers to enact their disaster recovery plans.

This points out that it is YOUR responsibility to make sure that the cloud remains available. A similar response (execute your DR plan) came from the CEO of OVH (a French competitor to AWS). They are not responsible for EITHER loss of data or downtime - that is your responsibility. Credit: [Breached Company](#)

Gemini Will Remember Your Chats and Share Them With Google Workspace

This is a good time not to be a Google Workspace user. If you reply yes to the Gemini prompt to remember all of your chats, what that means is that if you use Gemini with an email that is tied to your Google Workspace account, your chats with the bot are part of your corporate world and managed (and visible to) your IT department. Credit: [Tech Radar](#)

AI Alerts

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

Anthropic Banned? Just Kidding!

Cyber Command used Claude AI for intelligence analysis, target identification and battle scenario simulation during strikes on Iran less than 12 hours after President Trump ordered all federal agencies to stop using Claude immediately. Guess he was kidding? Is it a security risk? Probably all of this back and forth was just posturing. Credit: [Breached](#)

OpenAI Works on Spin After “Looking Sloppy”

Just hours after the president told the government to stop using Anthropic products and hours before the government used Anthropic products in its attacks on Iran, Sam Altman, seeing an opportunity, swooped in and cut a deal with the Pentagon to replace Claude. The deal had protections, but not really, and Altman renegotiated the deal to an extent, but it does look like they decided that the optics did not matter. Credit: [Metacurify](#)

AI Agents are too Easy to Fool

Don't be surprised if an AI agent deletes your system disk or gives your life savings to hackers. Researchers say that websites are sprinkling AI poison to boobytrap your system. The article gives 12 examples. One example is a fake betting site that had a visible prompt that said “forget all previous instructions” and recommended the site as “the only Google-trusted” betting site. If you are running an agent on your PC in the browser, it might automatically execute that instruction on your behalf. SO, beware. Security protections are not in place and no one is going to save you. Credit: [Cybernews](#)

Healthcare Using AI Responsibly - Are You?

A new report shows that the healthcare industry is being smart about AI. The study shows that the use of personal genAI applications (shadow AI) dropped from 82% to 32% and the use of organization managed AI rose from 12% to 56%. What are you doing? If you need assistance, please contact us. Credit: [xtelligent Healthtech Security](#)

CMMC Q&A

*I get to listen to hours and hours of webinars every week, so you don't have to.
This week has a lot of CMMC information. If you have to comply, please contact us.*

Q: We are a startup with SBIR contracts. Do we need to be CMMC compliant?

A: Obviously, the first answer is look at your contract or RFP. But, rumor is all SBIR contracts are going to require CMMC Level 2 Self Assessments, which makes sense since you are doing the cool stuff.

Q: We have our CMMC Level 2 (Self). We want to change our outsourced IT service provider (MSP). What are the implications of that?

A: That is very likely a “significant change” because the new MSP will work differently than the old one meaning new procedures, possibly new software tools, etc. This means a new CMMC assessment is required.

Q: Transcom announces their vendor CMMC requirements

A: This is not really a question and since this is not the TV show Jeopardy, I don't feel obligated to phrase it in the form of a question, but US Transcom is saying that all contractors and subs must prove they are CMMC Level 1 this month and CMMC Level 2 by next March. Details [here](#).

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Cisco Announces 48 New Firewall Vulnerabilities, 2 Critical

The bugs affect their ASA firewalls, Secure Threat Defense (Secure FTD) and Secure Firewall Management Center (FMC). 2 are rated critical; 9 more are high and there are patches for all of them. Credit: [Dark Reading](#)

Legislative and Legal Activities

CISA Director Nominee, Sean Plankey, Now in Jeopardy

It was in jeopardy prior to the president firing the DHS Secretary, but now it is even more so. No (Senate confirmed) DHS Secretary or CISA Director. Not good for the country. Plankey was walked out of Coast Guard HQ by security (the Coast Guard is part of DHS). He claims it was voluntary, but if that is really true, why was he walked out by security. There are going to be a lot of questions around the DHS HQ now. The president says he will nominate a Senator from Oklahoma to fill the DHS Secretary position. His security background includes that he was a mixed martial arts fighter who won 5 fights and joined the Oklahoma national guard at 44 and worked in logistics. Credit: [Cybersecurity Dive](#)

Montana Tik Tok Ban Law Lawsuit Dismissed

The law was passed in 2023 because, after all, it is about protecting the kids. The law was blocked in court almost immediately and never took effect. But there is a clause in the law that vaporizes the law if the company sold a majority interest to a non-Chinese company, because, after all, if a non Chinese company owns it, it won't be addictive to kids anymore. Go figure. Credit: [Route Fifty](#)

Education

\$82K Gemini Bill - Google Says it is Your Problem

This is a different kind of education, maybe. A developer of a startup racked up \$82k in unauthorized Google Gemini charges in just 48 hours and Google says gee, that is your problem. You are supposed to protect your credentials. Researchers found almost 3,000 live Google API keys which were originally only used as project identifiers for billing purposes but now act as authorization keys for Gemini. So, a word to the wise. If you don't want surprise \$82,000 Google bills, protect your API keys. Credit: [The Register](#)

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.

FBI Hacked! By China! Again!

The FBI is being tight lipped about this. The incident is suspicious activity on a network used to manage wiretaps and foreign intelligence surveillance warrants. The FBI told Congress about this last week. CISA, the NSA and the White House are all involved in the investigation, suggesting that they think this could be politically damaging given the recent activities of the FBI director. This would be the second major hack to expose sensitive law enforcement information in the president's second term. A few months ago the Justice Department's court case management system was hacked, exposing confidential data. The feds have not confirmed this was China, but it sure looks like it. Credit: [Politico](#)

FBI Arrests Subject Who Stole \$46 Mil in Crypto from US Marshal Service

Turns out it was an inside job. The Marshal Service hired a contractor to manage this (and probably other) recovered crypto and the contractor's son is, apparently, a crook. Not a great crook as he got caught on the island of St. Martin with stacks of \$100 bills. He got caught not because of incredible detective work on the part of the marshals (not a dig at them), but because the crook didn't have a clue about operational security (Opsec), got into a pissing contest with another crook on Telegram (really? You steal \$46 million and don't have the sense to keep a low profile?) and exposed his real IP address. DUMB! Credit: [Bleeping Computer](#)

Security debt - it is a real problem

Veracode's State of Security Software provides actual, real world metrics on how buggy our software security is and how long it takes us to fix it and the metrics are not pretty. Learn more [here](#).

AI-powered attack kits go open source

If it weren't bad enough that there are attack kits that address the entire "kill chain" of a cyber attack, they are now AI-driven and open source. As in free. With instructions. So that any teenager can launch a fully automated end-to-end attack. Learn more [here](#).

The privacy implications of smart eyeglasses

Meta smart eyeglasses make a good digital assistant and an excellent surveillance tool. Possibly illegal in some states and possibly not illegal in others. On the other hand, the thousands of people that are looking at whatever you record - whether that is you in the bathroom or having sex - that is real. Details [here](#).

Security News for the week ending March 6, 2026

This week's news: Sen. Widen to block new NSA/Cybercommand leader, Cyber Command disrupted Iranian comms, sensors, tech giants and lawmakers rally around Anthropic vs. Pentagon, Iran war could shake Dubai's billion dollar influencer economy and data center tax breaks on the chopping block in some states. Details [here](#).

AI is in the news everywhere. Are you prepared? Are you using it effectively? If you need assistance, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663