

September 6, 2026

If You Don't Want to be Scared, Don't Look at This Graph

CVEs are, basically, reported vulnerabilities or bugs. Most vulnerabilities are not reported but it is a trend nonetheless. Historically, we have been growing about 4,000 more reported vulnerabilities a year. Look at 2026's estimate and, I predict, this number is low. As of August we are already at 57,000 (actual data), which puts us at about 19,000 more vulnerabilities reported in 8 months than all of last year. Don't be surprised if this year ends at 80,000 or 90,000. SEE THE GRAPH BELOW.

Please check out our blog at [HTTPS://TCPS-BLOG.COM](https://TCPS-BLOG.COM)

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.

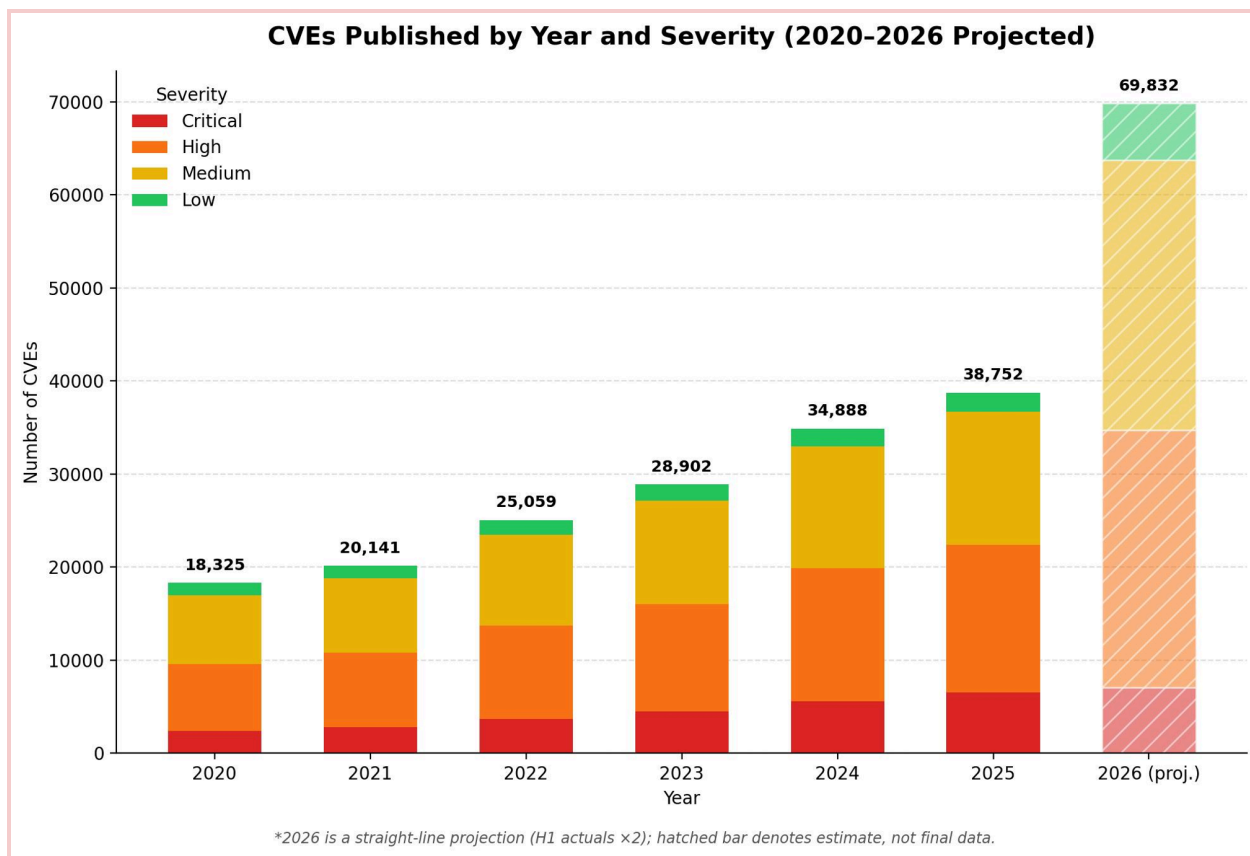
Video Blogs

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

If You Don't Want to be Scared, Don't Look at This Graph

CVEs are, basically, reported vulnerabilities or bugs. Most vulnerabilities are not reported but it is a trend nonetheless. Historically, we have been growing about 4,000 more reported vulnerabilities a year. Look at 2026's estimate and, I predict, this number is low. As of August we are already at 57,000 (actual data), which puts us at about 19,000 more vulnerabilities reported in 8 months than all of last year. Don't be surprised if this year ends at 80,000 or 90,000.



FBI Probes Service Selling 153 Million Drivers Licenses

It appears that this is a warning from many people, including me, coming true. The images appear to be from an identity verification service based in Louisiana. This is what happens when the government forces web sites to “verify” users. The forum selling the data is in Russia so while the FBI is welcome to “investigate”, it is not likely that they can stop the selling of the data. Some of the IDs list as their source “CDL”, presumably commercial drivers licenses, others are labelled “CAC”, likely referring to a form of government employee security cards. The hackers say they have been stealing the data for more than a year. The number of records keeps increasing - not clear why. Here are the current counts.

Categories	
Drivers License	153,347,439 records
Identification Card	10,335,678 records
Uncategorized	5,092,107 records
Travel Documents	1,924,144 records
International DL/ID	1,379,886 records
Medical Cards	579,201 records
Common Access Card	429,314 records
Residence Card	91,873 records
Employment Authorization	77,155 records

Credit: [Brian Krebs](#)

UPDATE: The company is being identified as IDScan, based in Louisiana. The hackers seem to be adding about a half million ID documents a day, suggesting they are still stealing data. Or else, they have already stolen so much data that they are still processing it. People who have seen the data found their own data in the database, increasing the odds the breach is real. The FBI is investigating and the company has not returned requests for comments, but recently their web site went offline and now there is a comment on their web site about it. Among the licenses in the database is Pete Hegseth's. The DoD is 'investigating'. Credit: [Tech Crunch](#)

Florida and Texas Move to Block Flock Cameras Over Privacy

You might not list Florida or Texas as one of the most left leaning states, so you would not expect them to be anti police or anti surveillance, but, apparently, politics makes strange decisions. Florida's Department of Transportation says it is no longer going to use license plate readers such as Flock and the state has 30 days to remove the tech. Governor DeSantis, a staunch Republican, said that the tech was "out of control". Texas, last week, ordered state agencies to stop funding Flock cameras. This comes as citizens are going after Flock devices and destroying them, they are so angry. The Flock brand, in particular, has become radioactive and, as a result, politicians, in an election year, need to at least pretend to be concerned. Will they change their mind a week after the elections? Only possible if they are still in office.

Credit: [Tech Crunch](#)

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>

OpenAI, the Most Sued Company in the World, Adds a Couple More

Total exposure is more than \$3 billion. There are 41 active or resolved cases. Many Worlds 2T Innovations added to that mix on August 30th. Patent infringement. Filed in the Eastern District of Texas, the most patent holder friendly court in the country. These patents, five of them, were filed as far back as 2014 and as recently as last year. Some of these patents go back to provisional patents dating to 2011. It is unclear how strong they are - software patents are notoriously weak - but I am sure the lawyers will get rich. If they win, well, that could be a problem for Mr. Altman. Credit: [AI Lawsuit Tracker](#)

Lutnick Says They Have Kissed and Made Up with Anthropic

This was announced right after the court sided with Anthropic and gave them summary judgement that the supply chain risk designation was revenge. No evidence this is related and Anthropic is still suing the government, but Howard said we are all good again. Credit: [CNBCTV18](#)

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.

Honeywell Settles False Claims Act Charges for \$2 Million

While there are not a lot of details available, the DoJ says that between April 2020 thru December 2023 they said they were compliant with the requirements of DFARS 252.204-7012. Apparently the government disagrees. This was a whistleblower suit and the former employee got \$375,000. Details on our [FCA settlement page](#).

Is the CMMC Phase 2 Pause a Win for Industry?

The short answer is no. Here is why. It is a way for the government to balance the budget without raising taxes. While False Claims Act settlements have been quiet this year, magically, during the "pause", it is heating up. If you don't have a third party certification then the attestation that your CEO makes on SPRS is completely on him or her. If the CEO ever pissed off an IT person during their tenure then that person may make a false claim case *Qui Tam (on behalf of the government)*. The most recent settlement was small. The "relator" (which is a legal term for the person you pissed off) got around \$350,000 plus another \$300,000 in legal fees. That, of course, does not include the \$2+ million fine, your legal fees and a requirement that they cannot take these costs off on their taxes. So, if you like spending money on lawyers, like giving the government cash and like having your name in the headlines at the DoJ, then, yes, this pause is good for you. Assuming none of these are true, then, no, it is not a win. Oh, don't forget, it looks like the DoD wants to ADD more requirements after the pause, not remove requirements.

**** REMINDER** 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.

Reference

Nothing to report

Software and Hardware to Check Out

Anthropic is Rolling Out Zero-Retention AI Safety Monitoring for Enterprises

It won't happen until this fall, but it is called Enterprise Frontier Safeguards (EFS). Data will be stored in the CUSTOMER'S cloud environment, with zero retention at Anthropic. Apparently, AI vendors are hearing from customers that they do not trust their vendors' security and privacy practices. Perhaps others will follow. Credit: [CSO Online](#)

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

Part of the False Claims Act is Qui Tam - Is It Legal?

Under many False Claims Act cases is the principle of Qui Tam. Under Qui Tam a whistleblower can file a suit on behalf of the government. Once the lawsuit is filed the government may take over the lawsuit if it wants. Not surprisingly, the people who are being sued are not fond of that. The 11th Circuit Court of Appeals just ruled that it is legal and reversed a ruling from the Middle District of Florida. Whether the Supremes are interested in picking up the case or not is unclear. The 11th Circuit joins the Fifth, Sixth, Ninth and Tenth Circuits saying it is legal. Typically, the Supremes only pick up cases when there is a circuit split, which is not the case here. That means that this is not fully decided, but for the moment Qui Tam is still alive. Credit: [Ballard Spahr \(Law Firm\)](#)

Madison Square Garden (MSG) Sues Wired Over Breach Reporting

MSG needs some security help. This breach is different from the breach last year that compromised information on 131,000 employees and contractors. This breach happened a couple of months ago and ShinyHunters published about 45 gigabytes of surveillance data when MSG didn't pay. Wired reviewed the data and claims some nasty stuff in the data including that MSG was tracking celebrities' sexual orientation. MSG of course is unhappy about this reporting and did not deny the substance but said there were other fields in the data like names and addresses. They said, in the lawsuit, that the reporting would bring additional attention and possibly even more lawsuits than are already being handled and they would prefer to keep this on the down-low. Sorry, it doesn't work that way. Credit: [USA Today](#)

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.

Qilin Hackers Leak ATF Data

Since the ATF didn't pay the ransom, the gang leaked the data. The data posted exposes case files tied to criminal investigations and field operations. It even included forensic evidence. But not to worry, the system breached was the CALEA (wiretap) system, not the administrative network. It could expose witnesses, informants, evidence and ATF officers, but other than that, things are good at the ATF. Credit: [Cybernews](#).

Healthcare Attacks Can be Life Threatening

Two recent healthcare attacks bring home the dangers of cyberattacks. One company makes pacemakers and the monitoring of those devices is impacted. The other is a drug maker where hundreds of millions of patient records were exposed. Learn more [here](#).

White House Has a Half Baked Plan to Improve Public Water System Safety

The White House has, apparently (no details have been released) convinced some tech companies to give away software and services to help public water systems to improve their security, but only for six months. It is unclear what happens after that. Learn more [here](#).

China Says THANK YOU for US Export Bans

The plan was to make China kow-tow to US demands. Instead, it is making China not only less dependent on the US, but allowing it to better compete against US tech companies. Not exactly the desired result. Learn more [here](#).

Security News for the week ending September 4, 2026

This week's news: Hackers use Twitter's AI to run exploit campaigns, AI could make it easier for terrorists to build weapons of mass destruction, deputy arrested for using Flock to search for his girlfriend 2,000 times, while passkeys are good, they are not magic and EU and US to surveil drivers soon. Learn more [here](#).

The DoJ is ramping up False Claims Act (FCA) settlements. There was a lull for a few months but we are seeing more of these again. FCA settlements can cover a wide range of actions. Whether it is CMMC or Healthcare or tech - or anything else - the DoJ is going after folks who stretch the truth. If you need assistance, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663