

June 21, 2026

Claude Code Can Even Document the Code it is Writing for You

Starting today, Claude Code can capture work progress as an artifact, which turns Claude Code's work into live, shareable visual pages—including PR walkthroughs, system explainers, dashboards, and release checklists—that update themselves as your session works. Credit:

[Claude Blog](#)

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.

This week there is a new video on AI - it is here to stay. Lead. follow or get out of the way, because it is coming for you.

Security/Privacy Alerts

Nothing to report

AI Alerts

Check out our Certified AI Governance Leader Course at AIGIP.AI.

AI Adoption Correlates with Incident Frequency, Points to Need for Governance

Even organizations that have not been breached expect AI-related incidents in the near future. And being a Mac shop doesn't protect you. More than 20 percent of Mac shops have lost money or experienced a cyberattack because of their use of AI and more than half of those Mac shops expect an AI-related incident in the near future. If you don't have a robust AI governance plan in place, contact us. Credit: [Cybersecurity Dive](#)

White House Wants Anthropic to Block All Jailbreaks - They Already Have

Can you predict the future? Neither can Anthropic. So the solution is to flip off the power switch. Problem solved. Some people may not like that answer but if the government wants AI to be perfect, that is not going to happen. I assume that the government has also told OpenAI and Grok that they can't export their software either (Hint: they have not). Oh, wait, both of them are campaign donors to the president. Do you smell something fishy? Does it make sense to make AI safer? Sure. Will it ever be perfect? No. It seems like if that is the goal then everyone should have to play the same game. But this is Washington. Credit: [Wired](#)

White House Blacklists Mythos but Does Not Blacklist China's DeepSeek

The White House says that Anthropic's Mythos and Fable are national security risks and need to be taken off the market but China's DeepSeek is fine, even though they CONSIDERED blocking it. It goes to show how politics is intertwined with security. And AI security. The president is going to visit China soon. He figures that blocking this software would tick off Xi, so even though DeepSeek is a national security risk with high probability since it was actually distilled from Anthropic's software and possibly removed the guardrails in Anthropic's software, the president is blocking Mythos and not blocking DeepSeek. Politics. Credit: [Tech Radar](#)

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: How do we deal with a requirement for flash drives if we disable flash storage to comply with CMMC?

A: First of all, CMMC does not prohibit the use of flash drives but it does require a strong management of the use, if required. But, more importantly, there are a number of ways to get around the requirement for flash drives on IN SCOPE systems, if they are actually required for business purposes. Contact us to discuss.

Q: Do we have to explicitly approve all software that our users want to use and document our review of those tools?

A: Not under the current rules, but it will be required when NIST SP 800-171 Rev 3 becomes the standard, likely some time in 2027, so now is a good time to start dealing with that. Contact us if you need assistance or have questions.

Another False Claims Act Settlement for Lying About Cybersecurity Compliance

This time it is a small company with only a few contracts. Around 30 employees. If you think that being a small company with small contracts gets you out of compliance requirements, check out this settlement. \$500k to this company is like \$5 million to a bigger company. Note that the total revenue from the contracts in question was around \$650k, so basically, the fine is the entire contract value. See the details on our [FCA page](#).

Q: What constitutes a Collaborative Computing Device?

A: Besides the obvious like a Zoom Room device, others include devices like Siri and Alexa-type devices or even Siri-style software on your phone. **According to the DoD directive, they cannot be within the capture range of conversations that may contain CUI.**

Reference

Nothing to report

Software and Hardware to Check Out

Claude Code Can Even Document the Code it is Writing for You

Starting today, Claude Code can capture work progress as an artifact, which turns Claude Code's work into live, shareable visual pages—including PR walkthroughs, system explainers, dashboards, and release checklists—that update themselves as your session works. Credit:

[Claude Blog](#)

Important Issues/Patches

Cisco Reveals SECOND SD-WAN Vulnerability Being EXPLOITED in Two Weeks

I think it sucks to be Cisco right now. SD-WANs are supposed to improve security. Not always. The bug was discovered during internal testing but hackers still figured out that it was there before it was even disclosed. A successful use of this exploit would allow a hacker to overwrite any file on the attacked system. Not good. Credit: [Helpnet Security](#)

27 Year Old Bug Found in OpenBSD

This is a one line error from the time when OpenBSD was ported from FreeBSD in 1999, almost exactly 27 years ago. It was fixed last week, after being vulnerable to a simple authentication bypass attack. Proof of concept code is available. Credit: [Argus](#)

Legislative and Legal Activities

US Government's Anthropic Ban Was Never About an AI Jailbreak

On Friday, a few days after Anthropic released Fable 5, the government issued an obscure export control directive that banned non-Americans, including those in the US and also Anthropic employees, from accessing Fable 5 and Mythos 5. Was this an issue of national security? Or was it revenge over a rocky relationship with the government? This method sidestepped the courts, at least for now. The news organization Axios says that personality differences between Anthropic and the administration led to the export directive, rather than a technical issue with AI products. If true, this is a warning to all businesses. If you cross us, we will cripple you. Oh, what a coincidence. This happened as Anthropic is launching its IPO. Stay tuned. Credit: [Tech Crunch](#)

FCC Wants to Outlaw Burner Phones

Because, of course, we don't have enough government surveillance yet, so why not? The excuse is to crack down on spam callers but since the FCC cannot enforce a global law, it really will just require spammers to move offshore if they are not already there, so it won't have any impact on spam. But, it will allow the government to identify whistleblowers, journalists and other people that they don't like. That is likely the real, covert requirement. I assume that politicians will somehow exempt themselves from this rule since they are huge users of burner phones. Credit: [404 Media](#)

Education

AI Data Centers Just Got a Government Mandated Fast Track to Electric Grid

The Federal Energy Regulatory Commission just got mad at the folks that run the electric grid and told them to get their act together to shorten the lead time for new data centers to get connected to the grid. They don't have the authority to tell them what to do but they can tell them to publish what the rules are. Seems reasonable to me. Credit: [Tech Crunch](#)

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.

Hackers Have Built a Database of over 30,000 Working Fortinet Firewall Logins

Since every "hack" has to have a catchy name, this one is called Fortibleed. Fortinet says this is not a result of a bug in the software. I assume that means that owners have either been socially engineered or have chosen weak or default passwords. Given that Fortinet is a very popular brand, it is likely that hackers would be able to find easy targets. The simple fix is to either not make your firewall interface public (which is our recommendation) or if you have to make it public, only make it accessible to a specified very small list of IP addresses. Either of these are easy to do and why some companies don't do that is likely due to a knowledge gap. If you need assistance with this, please contact us. Credit: [Cybernews](#)

Even Billionaires get Breached

Billionaire Peter Thiel, co-founder of PayPal and Palantir, has an invite-only "secret society" called Dialog. Basically a group of like minded people who get together periodically to discuss stuff. Recent topics included AI disruption, World War III scenarios, cult-building and politics. What got leaked was the list of attendees of this year's conference, scheduled for August near Dublin, personal information of the rich (and wannabe rich, including government officials), predictions and a members-only matchmaking service. Embarrassing. Credit: [Cybernews](#)

Big Pharma Maker Novo Nordisk Hit by Breach

This is an example of smart hacking. Rather than installing ransomware, hacking group FulcrumSec instead stole 1.3 terabytes - 700,000 files - of very sensitive data and asked for \$25 million, which they did not get. BUT, they still have the data and can use and/or sell it. The attack was simple; a single compromised GitHub access token. Among the data stolen was source code, proprietary drug information including about drugs not yet released, employee, doctor and patient information, internal AI models and other information. Credit: [Quartz](#)

ShinyHunters Publishes 26 Million Madison Square Garden Records

The data includes ticketing data, customer account information and internal corporate documents tied to both the national champion Knicks and the New York Rangers Hockey franchises. The hackers posted more than 42 gigabytes of stolen data. Data stolen included facial recognition data that tied faces to perceived risks those people represented. Credit: [Data Breach Today](#)

N.Y. explains that you need to report breaches

An insurance company discovered that if you fail to report a breach the state will come after you and whack you for millions. If you are part of a regulated industry you likely have around 72 hours to report a breach or face large fines. Learn more [here](#).

China to spend \$300 billion to beat us at using AI

Just a part of China's strategy is to spend \$300 billion to connect data centers across the country with at least 80 percent of that using Chinese tech such as Chinese AI chips and network hardware and they plan to do that in two years. How do we compete with this? Learn more [here](#).

Acting CISA Chief Says What we All Know - Out Loud

Acting director Andersen said out loud what all security pros have been trying to get people to understand with very limited success. The bad actors are going to have some major wins impacting critical infrastructure like power, water and communications and that will be very painful to us. Learn more [here](#).

Security News for the week ending June 19, 2026

This week's news: FCC says Chinese routers are not a security threat if you are a large ISP using them, was Nancy Guthrie a wrench attack by proxy, this is why you must manage the security of your vendors (Klue), cPanel zero-day now being exploited and UNPATCHABLE vulnerability in older Apple devices. Details [here](#).

You have probably noticed that a lot of our content lately is AI related. There is a good reason for this. Whether you like it or not, AI *IS**** affecting your business. Ignoring it is not a workable solution. If you need assistance in figuring out how AI is going to change your work world, please contact us.***

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663