

May 24, 2026

Researcher Microsoft Ticked Off Releases Two Zero Days the Day After Patch Tuesday

Microsoft seems to have a way of ignoring security researchers which makes them understandably upset. Some of them seek revenge by releasing exploits on the day after patch Tuesday. There are two of them this month. YellowKey is a **PHYSICAL** attack on bitlocker which allows an attacker with physical access to the computer to unlock Bitlocker protected drives if they are set to auto-unlock on boot. While Microsoft is working on a patch, the more secure solution is to require a password or PIN to unlock or require a BIOS password to reboot. One more time, you get to choose between security and convenience. If you want maximum security, you have to tolerate a little bit of inconvenience. Credit: [Threatlocker](#)

Please check out our blog at <https://www.cybercecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybercecurity-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://cybercecurity.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

Researcher Microsoft Ticked Off Releases Two Zero Days the Day After Patch Tuesday

Microsoft seems to have a way of ignoring security researchers which makes them understandably upset. Some of them seek revenge by releasing exploits on the day after patch Tuesday. There are two of them this month. YellowKey is a **PHYSICAL** attack on bitlocker which allows an attacker with physical access to the computer to unlock Bitlocker protected drives if they are set to auto-unlock on boot. While Microsoft is working on a patch, the more secure solution is to require a password or PIN to unlock or require a BIOS password to reboot. One more time, you get to choose between security and convenience. If you want maximum security, you have to tolerate a little bit of inconvenience. Credit: [Threatlocker](#)

The other attack is GreenPlasma, which is a privilege escalation attack on a computer that is already compromised (meaning you already have a bigger problem). It does point out that

vulnerabilities in trusted components are now a key attack vector and will be more so with AI tools like Mythos. See the same link for information on GreenPlasma.

CISA Admin Leaked AWS Govcloud Keys on Github

A contractor for CISA exposed AWS Govcloud keys and credentials for other internal CISA systems. The archives exposed documents how CISA builds, tests and deploys software internally. The GitHub repository is named Private-CISA. Apparently it was not very private. It included internal credentials and files, cloud keys, tokens, plaintext passwords and other sensitive CISA assets. Credit: [Brian Krebs](#)

AI Alerts

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

Musk Loses Lawsuit Against OpenAI

Musk sued OpenAI saying that OpenAI conned him into giving \$38 million to the OpenAI non-profit and then attaching a for profit company to it and accepting tens of billions of dollars from investors to that for profit entity. He said he should get about \$150 billion for that. The suit also charged that Microsoft was an accomplice. The jury ruled in only two hours that Musk waited too long to file the suit and so neither OpenAI nor Microsoft had to pay. The jury's verdict was unanimous. That means that if Musk wants to appeal he would have to prove that he did not exceed the statute of limitations for filing, which may be hard to do. Credit: [Reuters](#)

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.

How do we secure in-scope containers?

Containers represent an interesting challenge as they share the host OS kernel. As a result we would classify them as a specialized asset and secure the host and the container together. That means hardening the host to CMMC standards and then securing the container. For example, make container images immutable, create new patched containers rather than modifying in service containers, never bake secrets into containers, etc. If you need assistance with this, please contact us.

DoD Releases New Version of the CMMC FAQ, now called Version 5

Version 5 is obviously the number after version 2.2, right? I suspect they had a reason to change the numbering scheme, but that aside, there is some good additional information there. You can find the document on the [DoD CIO web site](#).

New Information in CMMC FAQ v5

- The DoD provided some new guidance on what constitutes a significant change which would require a new assessment.
- How to handle joint ventures (JVs)
- If you EXCLUSIVELY handle PAPER CUI, you don't need a CMMC assessment, but you do need to comply with DFARS -7012 and other related details
- How to handle changes while maintaining CMMC compliance

- Clarification that complying with NIST SP800-88 cryptographic erase meets CMMC requirements

The “NEW” FedRAMP

If you use cloud services, those services must be FedRAMP moderate or FedRAMP moderate equivalent. Well, FedRAMP is changing. While DoD hasn't officially approved the changes, the FedRAMP program office is moving ahead full steam. The PMO will stop accepting new FedRAMP “classic” requests come September 30, 2027. In the meantime, FedRAMP authorizations are now FedRAMP Certifications and FedRAMP low is now FedRAMP Class B, FedRAMP moderate is Class C and FedRAMP high is Class D. While the Pentagon has not formally recognized FedRAMP 20x, we know of at least one DIB contractor who passed a DIBCAC assessment with a vendor that was FedRAMP 20x and NOT FedRAMP Rev 5 That vendor has several customers who passed C3PAO assessments with that same vendor. Hopefully DoD will make an announcement soon.

Reference

China Gets Creative With Power and Cooling for Large AI Data Center

China has come up with a very creative way to cool and power a 2,000 server AI data center. Mind you, 2,000 servers is small for a data center, still, if you can use that as a repetitive module, you could scale it up. The data center is **offshore** near Shanghai and it is **under water**. The data center is cooled by seawater **basically for free** and powered directly from an offshore wind farm. Very interesting and solves multiple problems we are dealing with. It would require restarting our cancelled offshore wind farms though. Credit: [Tech Radar](#)



Software and Hardware to Check Out

Google Just Killed Off Search to Control the Narrative

We have seen this coming. Now Google killed their baby. Google search will no longer provide links to other sites. Instead it will regurgitate whatever is in Gemini. If you are a company that depends on referrals from Google, you are basically in a world of hurt. Time to reinvent your marketing strategy. It just proves that Google was never out there to help you; only to help itself.

Credit: [Computing](#)

Important Issues/Patches

Another Cisco Zero-Day; This Time SD-WAN Bug Grants Admin Access

A broken daemon peering authentication enables unauthenticated admin access. The bug rates a score of 10.0 - you cannot get any higher. Once you have exploited the bug you can manipulate the SD-WAN's configuration. CISA says it is being actively exploited. Rapid7 discovered this while researching another previous SD-WAN vulnerability. Multiple other SD-WAN bugs are being actively exploited. Time to patch. Credit: [Data Breach Today](#)

Is Open Source Bug Free? AI Finds 18-Year-Old Bug in Nginx

I know I keep beating on this, but open source software has just as many bugs as any other piece of software of similar complexity. Researchers using AI have found four bugs in Nginx, including one heap overflow that has been around for 18 years. Even the commercial version of Nginx is vulnerable. The issue rates 9.2 out of 10. Credit: [CSO Online](#)

Legislative and Legal Activities

Nothing to report

Education

Shark Tank Personality Kevin O'Leary is Building an AI Data Center in Utah

The data center as proposed would raise the day time temperature in the area by 5 degrees and the night time temperature by up to 28 degrees. In the desert. It would consume more than double the state's current electricity use. The proposal generated so much backlash that the county commissioners decided that no comments were allowed at the hearing where it was approved. Even though more than a thousand people showed up. Apparently, all the officials cared about was the potential tax revenue, but likely the state gave the developers credit, so there might not be any tax revenue for years or even a decade. Credit: [Route Fifty](#)

Another Critical Industry Infrastructure Group Forms Private CISA Replacement

Similar to the conversation last week about critical infrastructure group of power, water and gas utilities forming their own CISA-like group, now we are hearing about telecommunications providers AT&T, Charter, Cox, T-Mobile, Lumen and others have formed the Communications Cybersecurity Information Sharing and Analysis Center or C2 ISAC. One more time, these companies that used to be able to rely on the government have decided to go it alone because they can no longer count on the government. Credit: [Cybersecurity Dive](#)

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.**

NYC Health & Hospitals Hacked; Affects at Least 1.8 Million

The New York City Health and Hospitals system says a **months long data breach** allowed hackers to steal personal data, medical records and fingerprints of at least 1.8 million people. It is the largest public health system in the country and provides care for people who are uninsured or receive Medicaid. It is one of the largest healthcare breaches this year. The City says the breach started at a third party vendor, who was not named. Credit: [Tech Crunch](#)

Trump (Mobile) Can't Catch a Break

Besides delay after delay in delivering the phone, first claiming it would be made in America and then not, claims that the \$500 phone is a repackaged \$139 phone sold at Walmart and an incorrect number of stripes on the flag engraved on the back, they now have to deal with a data breach. A YouTuber revealed that TrumpMobile.com is exposing the names, addresses and other personal data of everyone who preordered one of these phones. He says he can even place fake orders. The exposed database shows roughly 30,000 total orders, the data from which is now, basically, public. Credit: [MSN](#)

Microsoft and others likely to break bug patch count this year

This month Microsoft patched 130 bugs; last month it was 173. Both of those numbers are much higher than usual. Likely, this is because Microsoft and others are using AI tools (Microsoft just announced an internal AI bug hunting tool called MDASH). Expect bug counts to get even higher, which means your patch work is also going to grow dramatically. Be prepared. Read the details [here](#).

Microsoft secure boot key to expire next month

The first of several encryption/signing keys that Microsoft uses to secure software that was released 15 years ago (the key was, not the software) is going to expire next month. That doesn't mean that your computer won't work, but some software that is signed with a new key won't work and you won't get all updates - if they need these new keys. For most PCs this update should happen in the background, but at least one of my PCs is requiring some manual hand holding. See how to check [here](#).

FTC warns big tech about the effective date of the "Take it Down" law

If you allow users to post content (like say Facebook and Twitter do), then this law impacts you. You have 48 hours to take down offensive content after being requested to and you have to make it easy for people to make the request. This is going to be really hard for the big guys and a pain for the small ones. Learn more [here](#).

Security News for the week ending May 22, 2026

This week's news: active bomb found underwater attached to Mobile, AL's water supply dam, Poland directs officials to ditch Signal for supposedly secure Polish alternative, America's largest Bitcoin ATM operator files for bankruptcy, Congress wants answers; CISA wants to stop the bleed from Github creds leak and Ken Paxton (Texas AG) sues Meta over lying about WhatsApp privacy. Read the details [here](#).

This reality is becoming clearer by the day. The tools and techniques you used pre-AI are not going to protect you today or tomorrow. If you are all over this then congratulations. If you are wondering what to do, give us a call.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663