

July 19, 2026

Microsoft Says Expect More Patches so Buy Our Expensive Automated Patching Tools

The story is valid. AI is definitely helping them find more bugs and given the amount of code, this won't end anytime soon. But the fact is that Microsoft's automation tools are not free (with the exception of the deprecated WSUS which has security holes) and there are many third party tools that do similar things, also not free. But you have to have the staff to manage these tools and they are definitely not free. Credit: [The Register](#)

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.

This week we added a video on what the DoD 60 pause of CMMC Phase 2 means. Check it out at the link above.

Security/Privacy Alerts

Researcher with Beef Against Microsoft Drops 9th Zero Day

Researcher Nightmare Eclipse is "unhappy" with how Microsoft has treated him and has repeatedly released zero-days, typically ON patch Tuesday or the day after to maximize Microsoft's pain. The vulnerability is called Legacy Hive and it is a local privilege escalation bug. It is the 9th zero day he has released in three months and was released hours after patch Tuesday. Maybe Microsoft ought to make peace with the guy. Credit: [Data Breach Today](#)

OpenSSL HollowByte Bug Can Take Out a Server with 11-Byte TLS Requests

The bug was patched last month with no CVE or notice that the webserver running OpenSSL was vulnerable to a denial of service attack. It did not even include a Changelog entry and, when exploited, it kills the process until it is restarted. Fixes are available for multiple versions of OpenSSL. Credit: [The Hacker News](#)

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.

Illinois Governor Signs Major AI Safety Law

While the president issued an executive order threatening to go after states that create AI laws, that does not appear to have slowed down the rate of state AI laws. Governor Pritzker signed a bill that they say creates the strongest framework for AI safety, transparency and accountability. The new law, known as The Artificial Intelligence Safety Measures Act, requires the largest AI developers to identify, disclose and mitigate risks associated with their systems, while providing for independent oversight and protections for workers who report safety concerns. It takes effect on Jan. 1, 2027. Credit: [Route-Fifty](#)

Researcher Poisons Open-Weight AI Model for Less Than \$100

Well, that is not too comforting. It took the researcher about an hour and cost less than 100 bucks. It only took ten training examples for the code output by the model to become reliably vulnerable to remote code execution. Credit: [The Register](#)

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 are the implications of the DoD PAUSING CMMC PHASE 2 ONLY for 60 Days?

The short answer is that we don't know, but the current phase, phase 1, is NOT paused, meaning they likely have no problem with the CMMC security requirements and only want to try and lessen the burden of the audits themselves. In addition, the Pentagon did not say stop doing third party assessments and it did not direct primes to not require third party assessments. Check out my podcast on the issue for more details. You can find it [here](#).

Q: What do we need to do to make sure we stay in compliance with CMMC after our assessment?

A: Fundamentally, you need to make sure that everything you say you are going to do in your SSP you are actually doing. If the SSP says that you **shall** do something every month, you actually need to do it every month and document that fact.

Q: Does the 60 Day CMMC Phase 2 Pause Mean That We Don't Have to Worry About Third Party Assessments of our Compliance?

A: Actually, not true. It is worse. Kirsten Davies said earlier this week ***"We also have the ability at any time, based on contractual regulations, to step in and conduct in-person assessments or documentation assessments of our defense industrial base as well,"***. These assessments are DIBCAC assessments which are much more comprehensive than a C3PAO assessment because they are not limited to just the 320 assessment objectives in NIST SP 800-171A. Be careful what you wish for. Credit: [Defense Scoop](#)

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Microsoft Says Expect More Patches so Buy Our Expensive Automated Patching Tools

The story is valid. AI is definitely helping them find more bugs and given the amount of code, this won't end anytime soon. But the fact is that Microsoft's automation tools are not free (with the exception of the deprecated WSUS which has security holes) and there are many third party tools that do similar things, also not free. But you have to have the staff to manage these tools and they are definitely not free. Credit: [The Register](#)

Microsoft Patches 622 Bugs in this Month's Patch Tuesday

Two are being actively exploited and a Bitlocker bug was disclosed. The Bitlocker bug, which was talked about last month but apparently not officially disclosed, requires physical access to exploit, so it is relatively low risk. Expect more patch Tuesdays like this. Details at [Security Week](#).

SonicWall Patches SMA1000 Bugs Exploited in Zero-Day Attacks

SonicWall warns that threat actors have been exploiting two SMA1000 vulnerabilities, tracked as CVE-2026-15409 and CVE-2026-15410, in zero-day attacks and urges customers to install the newly released security updates. One bug rates a 10.0 and the other rates a 7.2. SonicWall is investigating multiple incidents. Credit: [Bleeping Computer](#)

Legislative and Legal Activities

Nothing to report

Education

Courts Rule on Tracking Tech - Beware

Four courts. Five rulings. Three weeks. It kind of gives a bit of a picture. Which defenses worked and which ones did not. The issue is sharing tracking data with third parties and specifically what data. Was it what the person was searching for and some form of identifying information? Part of this hangs on what lawyers have loved and the courts are using it to hang them. ***We collect "some stuff" and we use it "some way". You approve, right?*** These courts are saying you have to be more specific. Even if you are not an attorney, this can give you guidance about what to talk to your attorney about. The link provides recommendations on what to do both before you get sued and after. Details at [Fisher Phillips \[Law Firm\]](#).

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.**

German Firm Files for Bankruptcy After Cyberattack

While not that frequent, we do hear of a number of cases of companies shutting down after a cyberattack. German textile company ZEGO said that a March cyberattack that shut down production for 6 weeks is causing the company to close. Credit: [The Register](#)

Coca-Cola Suspended Production at Fairlife Dairy

Coke is in a lot of businesses, including dairy. According to a filing with the SEC, Fairlife was hit by a ransomware attack and it affected its production systems. Fairlife by itself does \$4 billion a year in sales. They didn't say when they would resume production. Credit: [Tech Crunch](#)

The Internet in Europe is Undergoing Change

While this is now happening in Europe, it could come here. The European Parliament voted to allow tech companies to legally scan your messages to look for content that they think you should not have and the European Commission wants to ban social media completely for kids under 13 who are not under the supervision of a caregiver, whatever that means. While their motive is good for all of this, my guess is that the implementation will be less so. Government lawyers do understand side effects. Learn more [here](#).

FTC Ruling May Terminate EU Data Transfers

The US and EU have had a long (and litigious) history of how to transfer data from the EU to the US legally and it looks like this just got a lot more complicated. With the recent Supreme Court ruling that the president can fire independent agency staff at will, there is, basically, no such thing as an independent agency and that word is mentioned over 250 times in the current EU-US data transfer agreement. The EU is now being sued to cancel that agreement and the alternative (standard contract clauses and binding corporate rules) is almost as rocky, so if you transfer data, this is something to watch. Learn more [here](#).

Another Appeals Court Agrees that Border Agents Can Search Your Phone at will

No reason needed as one soul unfortunately found out. On the other hand, he had child porn on his phone. Not smart. This applies to corporate travellers, lawyers, anyone. And, it covers anything electronic - phone, table, flash drive, laptop, external hard drive. Anything. Learn more [here](#).

Security News for the week ending July 17, 2026

This week's news: AI camera triggers \$1,200 fine for phone on your lap, New York state signs first moratorium on data centers, Grok uploaded entire repositories including secrets like passwords and keys, Russia to launch Starlink competitor within days and federal tool to block non-citizen voters catches citizens. Learn more [here](#).

Let's assume that you use electronic devices at your company like phones, tablets and computers. Let's also assume that you don't have a bunch of IT folks sitting around doing nothing. Expect to be a lot busier for the foreseeable future as Microsoft released 3 times as many patches this month as ever before and Adobe is shifting to two patch Tuesdays a month. Are you prepared for this? Also assume that hackers are going to be able to figure out how to exploit the underlying bugs in record time. Finally, assume that they will use AI to attempt to break into your company's computers 24x7x365. Are you prepared for this? Give us a call.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663