

October 18, 2026

OKAY, This is Getting Out of Hand

Patch Tuesday was this week and Microsoft patched even more bugs than their earth shattering almost 1,000 bugs they patched last month. While not all of these bugs are earth shattering, assume that some of them are and further assume that the hackers are already looking through them to figure out which ones to use to attack you. **See details 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://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

OKAY, This is Getting Out of Hand

Patch Tuesday was this week and Microsoft patched even more bugs than their earth shattering almost 1,000 bugs they patched last month. While not all of these bugs are earth shattering, assume that some of them are and further assume that the hackers are already looking through them to figure out which ones to use to attack you.

ARE YOU READY? IS YOUR PATCH MANAGEMENT UP TO THE TASK?

Also assume that these number trends are what each responsible vendor is seeing also.

Are you using AI to look for bugs in software that you are writing? Have you asked your vendors if THEY are using AI to look for bugs in their software?

If you need assistance, please contact us.

Here is what Microsoft's monthly patch count looks like this year. Do YOU like the trend?

2026	Bugs Patched	
January	112	
February	59	
March	80	
April	167	
May	139	
June	200	(which was a record)
July	570	(Another record)
August	400	
September	965+	(again a record)
October	1,411	(A new record)

Credit: [Brian Krebs](#)

\$86 Million + Stolen From Crypto Hardware Wallets With Backdoors

Ledger is a company that makes hardware "wallets" that are used to store, hopefully securely, cryptocurrency keys. Unfortunately for at least 300 Ledger customers, that did not turn out to be true. This is not a super sophisticated cyber attack. A small number of wallets (so far) were tampered with in the supply chain somewhere. It appears that a chip and an antenna were added to the hardware after leaving the factory and before reaching the customer. Poof, the hackers now had access to the secrets in the wallets and stole tens of millions of dollars of crypto. Very old school attack. Credit: [Web 3 is Going Great](#)

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>

OH, Crap (or some other word). AI Agents Navigate Unfamiliar OT Systems in 16 Minutes

Historically, when humans were trying to navigate really obscure operational technology (OT) systems like power plants, dams, water delivery and the like, the fact that all of these systems were different and not like IT systems was a barrier. Booz Allen tested this theory in a closed lab. In their tests, AI models met every objective over eight different scenarios and compromised an industrial control network in about sixteen minutes. That means any strategy for protecting critical systems, both in industry (like manufacturing and logistics) as well as in critical infrastructure, that depends on hope that attacking them is too hard is DOOMED. In fact, the OT world might be the perfect target for several reasons - their cybersecurity practices match those of IT from 20 years ago, many of the systems are years if not decades old and so can't implement modern security practices and evidence is that many critical systems don't even implement basic cybersecurity hygiene. If you are dependent on hope as your strategy, that is probably not going to work well in the long term. Credit: [Security Week](#)

Accenture is Telling Employees That their AI Budget is \$29 a Month

There are a lot of caveats here, but here is the core. A company that has been spending as much as a thousand dollars a month per employee on Claude is saying hey, wait a minute, let's justify the spend. This is the same company that tells its clients to spend millions on AI. Not at all unreasonable. Corporate is saying they will fund the \$29, which is enough for some basic

chat accounts, but if you want to spend more, you need a charge number to charge it against. That means it is being charged to a customer or the department. While this sounds draconian, actually, this is the way consulting companies always work - you either self fund work (through an internal project or a customer) or you don't do it. Many companies got high on the AI Kool-Aid ® but then realized they had no strategy or governance around their use of the tech. If that is you, contact us. Credit: [404 Media](#)

This Should Concern You - B of A Hired 1,000 Contractors to Fix the Bugs AI Found

AI is finding bugs that have been around, in some cases, for decades. It is not inventing bugs but it is showcasing how horrible the security of most commercial software is. This month's Microsoft patch fest patched TEN TIMES (or more) the number of bugs they patched pre-AI. Does that mean that their software all of a sudden got buggier? NO. Bank of America had to hire 1,000 contractors to fix the first tranche of bugs that Anthropic Mythos found in their software. They spent **more than 100 million dollars** on that project. Those 1,000 people are in addition to the 3,000 people they already had. What does this mean for small companies and startups? Or companies that would rather not spend the money. After all, if you read the fine print you agreed to when you started using the software, your decision to use the software and all liability for damages is on you. ***That means that if the software is buggy and you are hacked, your customers WILL sue you and you and only you are liable for the breach. Your software vendor is not even partially liable (there are some rare exceptions, but generally, this is true).*** Are you talking to your vendors about this? If you need assistance, please contact us. 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.*

**** 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

Nothing to report

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

11th Circuit Says Georgia Can Force Everyone to ID Themselves to Access Social Media

Georgia already has a law that requires people to ID themselves to access adult sites but now everyone will need to ID themselves to access their Twitter or Snapchat accounts. The law requires commercially reasonable steps, whatever that undefined term means. There is a bit of a circuit split and the court didn't really rule on the totality of the law (typical), so there are still lots of potential challenges, but will Georgia residents be happy if they have to upload a government issued ID in order to look at their Instagram account, if that is what they do. It is also unclear what the platform strategies are going to be. Could be a very light touch and wait for the AG to try and sue them or it could be a very heavy touch and wait for the voters to impeach the governor. Stay tuned, this is not over.

Export Controlled Data and Cyber Incident Response

If you have cyber insurance, most likely you are required to use your insurance company's incident response team. Many times that team is offshore. If you have data which is export controlled or is DoD data (CUI), that can be a problem. It is best to discuss this with your insurance carrier beforehand if this applies to you.

Education

Russia Has Built Drones to Cut Through Electric Power Towers to Cause Blackouts

Reports say that the drones have an explosive charge in their wings which is designed to cut through metal and topple power line towers. This will cause local blackouts and as we have seen in the US, potentially major fires, and take days if not more to fix. Could other countries adopt this? Would this cause panic in the civilian population? Is it considered a war crime? Assume we will see more use of tech against critical infrastructure. Key point here is that this doesn't require millions of dollars for a terrorist to do this, so could Iran or North Korea, for example, launch this kind of attack against a major US power infrastructure? The short answer is yes. Credit: [Tech Radar](#)

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.**

More Cyber-Physical Attacks

This time it is supermarket refrigerators in France. They were hacked to raise the temperature to 122 degrees, ruining a large amount of food. There are several chains that use that brand of refrigerators and they were all affected. The losses were in the hundreds of thousands of dollars per store, in many cases. While maybe not related, retail stores in the Netherlands and Belgium suffered what they are calling a "cybersecurity incident" that aligned time wise with the French attack. We will see if these are linked. Credit: [Hackread](#)

Ukraine figured out how to decimate bots

While the administration is trying to get Ukraine to stop bombing data centers, among other places, the result appears to be clear that bot traffic is down significantly. This is good for the American public who gets to deal with the fake social media activity. Learn more [here](#).

Flock is having a bad PR day

I don't think that Flock has had a good PR day in quite a while. A researcher, using Flock's own data, found 300,000 Flock surveillance devices, which is a whole lot more than the 120,000 cameras they admit they have. It makes some people wonder what else they might not be telling us. Learn more [here](#).

What if the next attack isn't to set refrigerators on fire?

Last weekend attackers figured out how to compromise refrigerators in French grocery stores. Some refrigerators just set the temperature to 100+ degrees while other refrigerators caught fire. We saw this attack a couple of years ago on coolers on US military base PX stores. What if next time they decide to do something more spectacular? Learn more [here](#).

Security News for the week ending October 16, 2026

This week's news: Let's Encrypt leads in reducing TLS certificate lifetime, Flock Surveillance network is bigger than they admit, Chinese semiconductor exports dwarf US semi exports, ransomware hackers have a new technique to ensure payment and it is scary and White House threatened tech giants with H1-B suspension. Read the details [here](#).

Are you ready to deal with 1,000 to 2,000 bugs to patch a month?

The answer could be yes. Or no. But remember that Microsoft is only ONE vendor who has increased the patch rate by ten-fold. Patching for most vendors is NOT automatic and while some vendors will let you know that there are patches IF YOU OPEN THE SOFTWARE, most won't deploy patches automatically behind the scenes. If you have 50 pieces of software on each computer, however many computers you have, how solid is your patch system. Need help? Contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663