MY WEIRD PROMPTS

Podcast Transcript

EPISODE #216

The Secret Language of Security: CVEs and CrowdSec

Published January 12, 2026 • Runtime: 24:37

https://myweirdprompts.com/episode/cve-crowdsec-cybersecurity-explained/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, hosts Corn and Herman peel back the curtain on the invisible infrastructure that keeps the internet safe. Inspired by a listener's DIY OPNsense firewall project, they explore the "secret language" of cybersecurity: Common Vulnerabilities and Exposures (CVEs). They explain how the MITRE Corporation and a global network of Numbering Authorities coordinate to identify and score digital threats before they can be exploited by malicious actors. The discussion then shifts to the revolutionary power of collective intelligence, using tools like CrowdSec to create a "Waze for cyberattacks." By crowdsourcing threat data, individual users contribute to a global reputation database that protects everyone from automated botnets. From the high-stakes world of coordinated disclosure to the critical importance of maintaining open-source libraries like Log4j, this episode highlights how the digital world is moving from isolated silos to a massive, interconnected web of defense. Whether you are a sysadmin or a casual browser, you'll learn how the "trickle-down" effect of security protects us all.

DANIEL'S PROMPT

Daniel

I would like to discuss the international system for coordinating the reporting and patching of vulnerabilities, including the assignment of CVE codes. I also want to explore the crowd-sourced and open-source aspects of cybersecurity, such as tools like CrowdSec, and how collaboration between major operators and users can improve internet safety.

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am sitting here in our living room in Jerusalem with my brother. It is a beautiful day outside, the sun is hitting the stone walls just right, but we are about to dive into some of the darker, more complex corners of the internet.

Herman

And I am Herman Poppleberry. I have to say, Corn, I have been looking forward to this one. Our housemate Daniel has been doing some serious heavy lifting with his home network lately. He has basically turned our utility closet into a mini data center. He sent us that audio clip about his DIY firewall journey, specifically his move to OPNsense and CrowdSec, and it really got me thinking about the sheer scale of the coordination that keeps our digital world from falling apart.

Corn

It is funny you say that, because most people just see a little notification on their phone or laptop that says an update is available, and they click install without a second thought. They might even get annoyed by it. But Daniel is tapping into something much deeper. He is looking at the actual plumbing of cybersecurity. He mentioned CrowdSec and this international system of CVE codes. It sounds like a secret language, but it is actually the bedrock of how we handle vulnerabilities in twenty-twenty-six.

Herman

It really is. And I think it is important to start with that specific term Daniel mentioned, the CVE. It stands for Common Vulnerabilities and Exposures. If you have ever read a security advisory, you will see a string of characters like CVE dash twenty-twenty-four dash followed by a five-digit number. That is not just a random serial number. It is a unique identifier in a global catalog. It is the universal language of bugs.

Corn

So, it is like a social security number for a specific bug in a piece of software? Or maybe a VIN number for a car recall?

Herman

Exactly. Before the CVE system was established back in nineteen-ninety-nine, every security company had their own name for every bug. If Microsoft found a flaw, they called it one thing. If an antivirus company like Norton or Kaspersky found it, they called it something else. It was total chaos. You could not coordinate a response because no one was sure if they were talking about the same problem. Imagine a doctor trying to treat a patient, but every specialist uses a different name for the same virus. You would never get anything done.

Corn

That sounds like a nightmare for a system administrator. Imagine trying to secure a network when the reports are all in different languages, metaphorically speaking. So, who actually manages this list now? Is there a central world government for internet bugs?

Herman

Not quite a government, but a very influential non-profit called MITRE Corporation. They operate the CVE program, which is funded by the United States Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency, or CISA. But it has become a truly international effort. They do not do all the work themselves. They have what are called CVE Numbering Authorities, or CNAs. These are organizations authorized to assign these codes. As of early twenty-twenty-six, there are approximately four hundred CNAs across nearly forty countries, reflecting significant growth in recent years.

Corn

Wait, so companies like Apple or Google are their own numbering authorities? They get to decide when a bug in their own system gets a code? That feels a bit like the fox guarding the henhouse, doesn't it?

Herman

It could be seen that way, but the system is designed with checks and balances. If a researcher finds a bug in Chrome, they report it to Google. Google, acting as a CNA, assigns a CVE ID. They then have a period of time to fix it before the details are made public. This is where we get into the CVSS, or Common Vulnerability Scoring System. It is a numerical score from zero to ten that tells you how dangerous the bug is. A ten point zero is the digital equivalent of a five-alarm fire.

Corn

Daniel touched on this in his prompt. He called it a cat and mouse game. He mentioned that you do not want to tip off the bad guys by announcing a vulnerability before you have a patch ready. But he also mentioned he has reported a few vulnerabilities himself. How does an individual like Daniel fit into this massive corporate and governmental machine?

Herman

That is the beauty of the coordinated disclosure model. When a researcher finds a flaw, they usually agree to an embargo. They say, I will give you ninety days to fix this, and then I am going to publish my findings. This gives the vendor time to create a patch. If the vendor ignores them, the researcher might go public anyway to force their hand. It is a delicate balance. The goal is to get the patch to the user before the exploit becomes widely known to hackers. In 2025, we saw a high number of these disclosures, partly because the tools for finding them have become so much better.

Corn

I see. But what about the other side of Daniel's question? He was talking about tools like CrowdSec and the open-source aspect of this. It feels like we are moving from a top-down system, where big organizations manage the lists, to a bottom-up system where everyone's firewall is talking to everyone else's. It is more democratic, right?

Herman

That is a massive shift, Corn. CrowdSec is a perfect example of this. Think of it like Waze, but for cyberattacks. On Waze, if you see a pothole or a police officer, you report it, and everyone else on the road gets a warning. CrowdSec does that for servers. If someone tries to brute-force their way into Daniel's home server, his CrowdSec instance detects that behavior. It is not looking for a specific file or a known virus; it is looking at behavior. It sees someone trying a thousand passwords a minute and says, wait, that is not a human.

Corn

And then it blocks them locally, but what happens next? How does that help me?

Herman

It blocks the IP address locally using what they call a bouncer. But then it also sends a signal to the central CrowdSec database saying, hey, this specific IP address is acting aggressively. It is like a neighborhood watch where everyone has a high-speed radio. If a suspicious car is seen at Daniel's house, the whole neighborhood knows about it in milliseconds.

Corn

And then that information is shared with every other CrowdSec user in the world? Even people who do not know Daniel?

Herman

Precisely. It creates a global reputation database. If that same hacker then tries to attack my server, my firewall already knows to block them because Daniel's server already flagged them. It turns the vastness of the internet into an advantage for the defenders. Instead of one person fighting one hacker, it is a million firewalls fighting together. This is what we call collective intelligence, and in twenty-twenty-six, it is the only way to keep up with automated attack bots.

Corn

I love that analogy, but it makes me wonder about the second-order effects. If we are relying on crowd-sourced data, how do we know the data is good? Could a malicious actor use a tool like CrowdSec to get legitimate IP addresses blocked? Like, could I trick the system into thinking a major website like Wikipedia is actually a source of attacks?

Herman

That is a brilliant question, and it is the primary challenge for any crowd-sourced security tool. They use a consensus mechanism. A single report from one server is not enough to get an IP address globally banned. The system looks for patterns. It requires multiple reports from unrelated sources over a certain period. They also have a reputation system for the reporters themselves. If Daniel's server consistently provides accurate reports that are verified by others, his trust score goes up. If he starts reporting Google's IP addresses, the system will ignore him.

Corn

So there is a built-in filter for noise and malice. That makes me feel a bit better. But what about the big players? Daniel mentioned the big names like Norton and Kaspersky. Those are the traditional giants. They have huge research labs and proprietary databases. How do they feel about these open-source, community-driven tools? Are they collaborators or competitors?

Herman

It is a bit of both, but the trend is definitely toward collaboration. The traditional players still have a massive role because they can do deep-dive forensic analysis that a crowd-sourced tool might miss. They can take a piece of malware apart in a lab to see exactly how it works. But even the giants are starting to realize they cannot see everything. The sheer volume of traffic in twenty-twenty-six is so high that no single company can monitor it all. We are seeing more collaboration through organizations like FIRST, the Forum of Incident Response and Security Teams.

Corn

It reminds me of what we discussed back in episode one hundred and eighty-six, when we were looking at airport networking. The stakes are so high that you cannot afford to be an island. If one part of the system fails, it can cascade. Daniel's point about his DIY firewall is really about taking personal responsibility for a small piece of that global system. He is not just protecting his own photos; he is contributing to the health of the whole network.

Herman

Exactly. And that brings up a really important point about internet safety for the average person. Most of us are not going to be reporting vulnerabilities to MITRE or running complex behavioral analysis on our home servers. But we benefit from the work that people like Daniel do. When his server flags a botnet, and that information trickles up into the blocklists used by major internet service providers, my mom's iPad becomes a little bit safer. It is a trickle-down effect of security.

Corn

So, it is a pyramid. At the top, you have the formal systems like CVE and the National Vulnerability Database. In the middle, you have the big security vendors and the open-source communities like CrowdSec. And at the bottom, you have the billions of users who just want to browse the web without getting their data stolen. Is that a fair way to look at it?

Herman

That is a good way to visualize it. But the pyramid is becoming more of a web. The lines are blurring. For example, look at the Log-four-j vulnerability from a few years back. That was a flaw in a tiny, open-source logging library that almost every major corporation in the world was using. It took a massive, coordinated effort between independent researchers, corporate security teams, and government agencies to map out where that code was and how to patch it. That was a turning point. It showed that the security of the biggest companies depends on the quality of open-source code written by volunteers.

Corn

That is a bit terrifying, honestly. It means the entire global economy is resting on the shoulders of people who might be doing this as a hobby in their spare time. What if they just decide to stop?

Herman

That is why we are seeing more corporate funding for open-source security. Companies like Google and Microsoft are now paying developers to maintain these critical libraries. Ongoing efforts by the Open Source Security Foundation, established years ago, have gained more corporate funding in recent years. It is about making sure the foundation of the house is solid, not just the front door.

Corn

I want to go back to something Daniel said about the process of reporting a bug. He said it was very structured and that he got an incident ID and worked with the vendor's security team. That sounds very professional, but I imagine it can also be quite frustrating. What happens if a company just ignores a researcher? Or worse, what if they threaten them with legal action?

Herman

That used to happen a lot more than it does now. It is called the chill effect. But today, most major companies have Bug Bounty programs. They actually pay people like Daniel to find bugs. If you find a critical flaw in a major cloud provider's system, you could walk away with fifty thousand dollars or more. This has turned a lot of hobbyists into professional security researchers. It aligns the incentives. Instead of the researcher being a nuisance, they are a valuable partner.

Corn

It is a power dynamic shift. The individual researcher has the truth, and the corporation has the resources. The CVE system acts as a sort of neutral ground where they can meet. But what about the bad actors? Are they using the CVE list as a shopping list for targets?

Herman

That is the risk. As soon as a CVE is published, it is a race. The hackers are trying to write an exploit, and the users are trying to install the patch. This is why the time-to-patch is such a critical metric. In twenty-twenty-six, we are seeing hackers use AI to automate the creation of exploits based on CVE descriptions. It has shortened the window of safety from weeks to sometimes just hours.

Corn

That brings us to the AI side of things. Daniel mentioned he is seeing more AI-driven attacks on his logs. How is the defense keeping up? If the bad guys are using AI to find the holes, are we using AI to plug them?

Herman

We are. We are seeing the rise of autonomous cyber defense. There are systems now that can detect an attack, analyze the method, and write a temporary firewall rule or even a code patch in real-time without a human ever being involved. It is like an immune system that evolves as it encounters new viruses. The DARPA AI Cyber Challenge, which advanced the field a couple of years ago, really pushed this technology forward. We are moving toward a world where the defense is as fast as the attack.

Corn

Let's talk about the practical side for our listeners. If someone is listening to this and they are feeling a bit overwhelmed by the technicality, what are the key takeaways? Daniel is out there building his own firewalls, but what should the rest of us be doing to participate in this ecosystem of safety? Do I need to learn how to code?

Herman

Not at all. The most important thing is actually the simplest: enable automatic updates. I know it sounds basic, but when you see that a software update is available, it is often because a CVE has been issued and a patch has been created. By updating, you are closing the door that the international community worked so hard to identify. You are the last link in that chain of coordination.

Corn

That makes sense. You are basically benefiting from the entire chain of events we just described. From the researcher who found the bug to the CNA that assigned the code to the developers who wrote the fix. It is a global team effort, and your only job is to click okay.

Herman

Exactly. Another thing is to be aware of the devices in your home. We talk about this a lot, but the Internet of Things is a major weak point. Many of those cheap smart bulbs or cameras do not have a robust system for reporting vulnerabilities. They might not even have a way to receive patches. If you are buying a connected device, look for companies that have a clear security policy and a history of providing updates. If a company does not have a way for researchers to report bugs, do not buy their products.

Corn

And for the more tech-savvy listeners, like Daniel, what is the next step? Is it worth running something like CrowdSec on a home network? Or is that overkill for a regular house?

Herman

If you have a home server, a NAS, or any device that is exposed to the internet, absolutely. It is a great way to learn about the types of traffic hitting your network. You will be shocked to see how many bots are knocking on your digital door every single minute. And by running it, you are contributing back to the community. Your server becomes one of those many eyes we talked about. You are helping to protect everyone else. It is a small act of digital citizenship.

Corn

I love the idea of the internet being a community effort. We often think of it as this cold, mechanical thing, but it is actually built on these layers of human collaboration. People like Daniel, the researchers at MITRE, the developers at the big tech firms—they are all working in this weird, complex dance to keep the lights on. It is almost poetic when you think about it.

Herman

It is a fascinating ecosystem. And it is constantly changing. One thing I am keeping an eye on for the rest of twenty-twenty-six is how geopolitical tensions affect this. We are seeing more national-level vulnerability databases being created, which could fragment the global system. If countries stop sharing bug information with each other because of politics, the whole internet becomes less secure. The CVE system is one of the few places where the whole world still cooperates.

Corn

That is a sobering thought. It means that cybersecurity is not just a technical issue; it is a diplomatic one. We need to keep these channels of communication open, regardless of what is happening in the physical world. The internet does not have borders, and neither do the bugs.

Herman

That is exactly right. And that collaboration is our best defense. The more we share information, the harder we make it for the attackers. When a major operator like a big cloud provider shares their telemetry with a non-profit security group, the entire internet gets a little bit more resilient. It is about building a herd immunity for the digital world.

Corn

I think that is a really empowering thought. We are not just passive victims of cyberattacks. We are part of a global system that is actively fighting back. Whether it is through formal structures like the CVE or grassroots efforts like CrowdSec, the good guys are collaborating at a level that was unimaginable twenty years ago. We have the tools, we have the community, and we have people like Daniel keeping watch.

Herman

It is true. And I think Daniel's experience shows that you do not have to be a giant corporation to be a part of it. Even a single person with a curious mind and a DIY spirit can make a difference. By reporting those bugs and setting up his own defenses, he is contributing to the safety of the whole house, and by extension, the whole network. He is a node in the global defense web.

Corn

Well, I for one am glad Daniel is the one doing the heavy lifting on our home network. I will stick to asking the questions and making sure the coffee is hot.

Herman

And I will stick to reading the documentation and explaining the acronyms. It is a good system we have here. We all have our roles to play in this weird digital world.

Corn

It really is. I want to take a second to thank Daniel for sending in this prompt. It is a topic that is so easy to overlook because when it works, you do not see it. But it is literally the foundation of our digital lives. Understanding how these systems work makes the internet feel a little less like magic and a little more like a well-coordinated machine. It is a machine built by people, for people.

Herman

Absolutely. And to all of you listening, if you have been enjoying these deep dives into the weird and wonderful parts of our world, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other people find the show and join our community of curious minds. We are growing every week, and it is all thanks to you.

Corn

Yeah, it makes a big difference for us. You can find us, as always, on Spotify and at our website, myweirdprompts.com. We have all our past episodes there, including that one on airport networking, and a contact form if you want to send us a prompt of your own. We read every single one.

Herman

We love hearing from you. Whether it is a technical question about networking or something completely off-the-wall about the history of the internet, we are always ready to go down the rabbit hole. No topic is too weird for us.

Corn

I think we covered a lot of ground today. From the history of the CVE to the future of crowd-sourced security and the role of AI in twenty-twenty-six. It is a lot to process, but it is a journey worth taking. It makes you realize how much work goes on behind the scenes just so we can send an email or watch a video.

Herman

It definitely is. I think I am going to go check the logs on our router now. Daniel probably has some interesting new data to show me from the overnight scans. I saw a lot of traffic coming from a new range of IP addresses this morning.

Corn

Just make sure you do not break the internet before I finish my coffee. I have a few more things to look up before we head out.

Herman

No promises, Corn. No promises. If I find a zero-day, all bets are off.

Corn

Fair enough. Well, this has been My Weird Prompts. Thanks for listening, and we will catch you next time. Stay safe out there in the digital wild.

Herman

Stay curious, everyone. Goodbye!