

The Man Who Saved the Internet Yesterday

Charlie Warzel

On Tuesday, the world found out about two massive security vulnerabilities in PHP, a programming language that is used by roughly 70 percent of websites. The flaw was discovered by cybersecurity researchers using a frontier model from OpenAI. If they exploited it, attackers could gain full control of servers, stealing or copying anything inside or simply taking sites offline.

The PHP Foundation, the organization that maintains the programming language, had recently learned about the security flaws, but the disclosure was leaked on a forum before a patch could be released. What happened next was a frantic race with numerous participants: the foundation, which needed to create and release a patch; developers around the world, who would need to deploy it; and attackers looking to exploit these vulnerabilities in the interim. Matthew Prince, the CEO of the hosting company Cloudflare, [wrote](#) that in the 10 hours before the flaws were publicly announced, “we saw thousands of attempts to exploit it. That jumped to tens of thousands in the 45 minutes post announcement, hundreds of thousands within 2 hours, and millions now.”

Once the patch was released yesterday, websites everywhere went offline to implement the fix. These included government websites in Germany and Finland, some hospital and school websites in Europe, and international sites such as 4chan. During this race to secure the majority of the internet, I noticed one name [pop](#) up in [posts](#) on Reddit and X: Ondřej Surý.

“Explaining to my wife how there’s this one guy. And he alone is responsible for most of the world’s distribution of PHP,” a software developer named Ian Landsman [wrote](#) on X. “And if anything happens to this guy, that’s just it. Everyone is screwed.” He was referring to Surý.

Surý, who lives in Czechia, does not work for the PHP Foundation. But alongside his day job as director of domain-name-system engineering at the nonprofit Internet Systems Consortium, in a volunteer capacity, he maintains and helps automate patches for the coding language. His work, with that of just a handful of others, has allowed countless websites and organizations to fix these vulnerabilities quickly. Over the past 48 hours, he’s become arguably the unsung hero of the entire internet—despite the fact that the only compensation he receives is from modest donations. “Ondřej will save the internet today,” a user in the PHP Subreddit wrote.

I spoke with Surý today from his home about the unfolding AI-cybersecurity crisis, how the internet’s infrastructure is maintained by small crews of volunteers such as himself, and how it feels to go to bed after saving the web as we know it.

Our conversation has been edited for length and clarity.

Charlie Warzel: Explain to me what has happened in layman’s terms over the past 72 hours.

Ondřej Surý: Earlier this week, I got notified by the PHP project that there was a serious security vulnerability in the coding. On Tuesday, it became apparent that someone had leaked information about the upcoming vulnerabilities, and it was decided inside the PHP project that it needed to accelerate the release process from Thursday to Wednesday. This is when it became a little bit crazy, because now we were one day short suddenly.

Warzel: I want to try to put this into perspective: So basically, the PHP programming language that kind of undergirds the web is used by up to 70 percent of websites?

Surý: That's what I heard as well.

Warzel: So people search for cybersecurity vulnerabilities, not necessarily for offensive-attack opportunities but maybe just defensive opportunities. And someone found a vulnerability—that's not super abnormal. But the real issue here was how widely it was disclosed and the amount of time before people had to patch this, right?

Surý: Let me clarify that: It's the severity. The severity is unusual. Remote Code Execution is the most severe type of vulnerability, because the attacker is able to execute their own code on the server that's running PHP. That's why this caused such panic throughout the internet. As you said, if about 70 percent of websites are running PHP, the impact would be huge if attackers would actually be able to execute code on these servers.

Warzel: You said that despite the panic online, it has not been a crazy 48 hours. From the outside, that's surprising. I keep seeing people saying, *There's one person who is in charge of fixing this—and he's supporting himself through Patreon*. They may have been exaggerating, but there's some truth to that: Your work was single-handedly helping millions of people. How could this not be a crazy time for you?

Surý: There are a couple of reasons. One is that I've been doing this for a long time, over 20 years. A lot of the stuff that I do is automated. But the reason it was not crazy for me was that I actually don't have any system running PHP myself. So for me, it was like, sure, I feel a responsibility toward the users of the internet. It would be a crazy day for me if I was on a boat in the middle of the Adriatic Sea. That could happen. But I had time to prepare the packages.

Warzel: That's kinda wild.

Surý: And even without me, people would still be able to get PHP from other sources and compile it themselves. But it would be more complicated for everyone. And some people don't immediately have the skill to upgrade the PHP. What the PHP project did was release the source code for the language. What I am doing is preparing it into these things called packages that people can install on their servers. It's very convenient, and it's faster, and you can automate it and can install the same package over hundreds and thousands of servers, and you don't have to compile it. If I was not available, it would take more time; some of them wouldn't have the skills. Really, the thanks go to the PHP project that invited me into this secret cabal who knew about the vulnerabilities and had access before the public release.

Warzel: When you got invited, was it a real *Oh, crap* moment for you?

Surý: I'm in the stage of my life where I was like, *This is bad. It needs to be fixed*. But it doesn't cause panic, at least for me. It did cause panic for a lot of people. But you know, it was more like, *We have a situation, it needs to be solved, and this is how we do it. And I have time to properly prepare*. If I didn't have time to properly prepare, then it would cause a lot of stress. From where I stand, it was not stressful, because I'm doing this as a volunteer, and if I get hit by a bus, then it will be someone else's problem.

Warzel: Every time I dabble in writing about the world of cybersecurity and open-source software, I discover these groups of maintainers: people such as yourself who do this work because they care. Often, nobody knows their name. But is there a line of people who would take your place if, say, you *did* get hit by a bus?

Surý: I am actually thinking about contingency plans. And we are talking with Raphaël Hertzog from the software company [Freexian](#). My advantage is that I have a lot of expertise, and I know where to touch the thing to make it work. But Freexian has a lot of expertise, and they would be able to take over if anything happens.

People have been donating small amounts, and larger amounts, like crazy since yesterday. I would like to thank them all.

Warzel: Have the donations been overwhelming?

Surý: Not Silicon Valley levels of money, but I got a serious amount of contributions that I've never seen before. It's like one year of the contributions gathered over the past 24 hours.

[Matteo Wong: Read this website while you still can](#)

Warzel: What would have happened if this wasn't patched as quickly as it was?

Surý: A lot of things could have happened. The very basic thing is that there would be vandalism, that the sites would be taken down. And we are seeing this every day on the internet now. The other stuff that happens is that someone gets access and runs a botnet out of these devices. I would say it's mostly organized crime doing that now—it's not like a small guy in the basement doing this for fun. There are financial incentives for these people to sell the botnet services or to do the crypto-mining on these servers for a profit. And this still could happen, because it's not like everyone has patched and updated their PHP.

Warzel: I saw a post on X that said not all PHP releases are patched, and one-third of the internet is kind of permanently either broken or vulnerable. Is that correct?

Surý: That initial information is not correct. There are ways to patch even the old versions.

Warzel: So one-third of the internet is not permanently screwed. Okay.

Surý: No, that's not accurate. If people care enough, they are able to even update these old versions of PHP.

Warzel: It's a scary moment for cybersecurity. I've seen people online referring to this vulnerability and other AI-agent hacks as "[Black October](#)," and there's concern that defensive or attacking agents can find these vulnerabilities. There is this feeling that I am noticing from the cybersecurity community that their fears of a future where things are being exploited or discovered quicker than people can handle is coming true—that we are living in that moment. And then separately, there's a contingent of people who are saying there is an equilibrium here: If you have very persistent agents that are very good at identifying and exploiting vulnerabilities, you also have very persistent agents that are very good at defending against them.

Surý: What we've seen is that things have accelerated—that's absolutely right. The defenders are also able to use the large language models to find the vulnerabilities for themselves. I believe it boils down to the simple fact that IT infrastructure is often being taken for granted.

There's not enough priority and money going to properly maintain the IT infrastructure in various places. It's not only companies; it's also a lot of outdated consumer electronics that are going to be attacked. I kind of agree that everything's moving fast now, and it's taking a toll on the people who are defending the stuff. At the same time, maybe this is the turning point where we actually start caring about this.

[Ian Bogost: Invasion of the self-replicating AI-malware botnet](#)

Warzel: Do you feel like that will actually happen?

Surý: I might be wrong, but I'm an optimist that people will finally realize that we can't go like this forever. This has been a disaster waiting to happen for a really, really long time. And this is just one of the many wake-up calls that came and will be coming.

Warzel: I am amazed by how much the infrastructure in certain areas of the internet can hinge on one or two people. There is a fragility to all of this that is concerning. So what do you want to see?

Surý: When I started doing open-source, it was fun. And it kind of still is. But the environment has shifted. Open-source sometimes feels like exploitation. What I would like to see is to find a new model

where people working on open-source would be awarded for their work and the hours and hours they put into it from the people who most benefit from their work. I would like companies to realize that this is exploitation. Any exploitation is not sustainable. And it will end up badly if this continues, because the people doing the open-source will stop being motivated to actually do anything in the end.

Warzel: It sounds like you don't have an ego about all of this. But you did some work, and you helped out a tremendous amount of people in every corner of the world yesterday. How did it feel to go to bed last night after all of that, knowing the role that you played?

Surý: Well, my wife says that I'm emotionally dead, but I'm not. And it felt nice. Like, seeing my social network filling up with thank-you notes, and getting emails with thank-yous, that feels really nice. It puts some sense into what I do. I felt that what I do has a purpose.

Warzel: The whole internet appreciates your efforts. Is there anything that you would recommend normal people do at this moment to improve their internet hygiene?

Surý: I would recommend that they rely on the experts. That's what we all do in a crisis: We talk to experts and trust them. Rely on people, that people who take care of this stuff know what they are doing. And that's all we can do.