

DJI will pay \$30K to the man who accidentally hacked 7,000 Romo robovacs



On Valentine's Day, I brought you a story that's since made headlines all around the world: How one man, just trying to steer his DJI robot vacuum with a PlayStation gamepad, discovered an entire network of 7,000 remote-control DJI robots ready to let him peek into other people's homes.

To be clear, DJI had already begun addressing some of the related vulnerabilities before the man, Sammy Azdoufal, showed *The Verge* just how much he could access. But it wasn't clear whether DJI would pay him for his discovery, particularly after how it treated security researcher Kevin Finisterre back in 2017 – or how soon DJI might fully patch the additional vulnerabilities that Azdoufal discovered.

Today, we have some of the answers.

DJI will pay Azdoufal \$30,000 for one single discovery, according to an email he shared with *The Verge*, without specifying which discovery it's paying him for. Though DJI is not naming Azdoufal, it confirms to *The Verge* it has "rewarded" an unnamed security researcher for their work.

DJI would also not tell us which discovery it's paying him for, but says it has already addressed the extra vulnerability Azdoufal found where someone can view a DJI Romo video stream without needing a security pin. "We can confirm that the PIN code security observation was addressed by late February," reads a statement provided by DJI spokesperson Daisy Kong.

You might be wondering: *What about the vulnerability that seemed so bad we refused to describe it in our original story?* DJI tells me it's working on that one too: "We have also started upgrading the entire system. This includes a series of updates, which we anticipate will be fully implemented within one month."

DJI has also published a public blog post today about strengthening the DJI Romo's security, one where it continues to claim that it discovered the original issue itself, while also crediting "two independent security researchers" for finding the same problem.

There, DJI seems to be suggesting that everything's *already* resolved with the Romo: "Updates have been deployed to fully resolve the issue." But again, there wasn't just one vulnerability, and DJI told *The Verge* that it could take as long as another month.

In the blog post, DJI also says that the Romo already has ETSI, EU, and UL certifications for security – which may raise questions about how useful those certifications really are if one guy with Claude Code could access an entire network full of robovacs! – and that it will continue to test, patch, and

submit the Romo and its app to independent third-party security audits.

DJI writes that it is “committed to deepening our engagement with the security research community, and we will soon introduce new ways for researchers to partner and collaborate with us.”

<https://www.theverge.com/news/890982/dji-pay-sammy-azdoufal-robot-vacuum-hack-romo-security>