

Forum: [Hack Forums](#)

Thread: [I published a new blog post about a recent 0-day](#)

Under The Breach - April 30, 2020, 11:53 am

Hey guys, once again posting my blogs here too

New blog - The Chronicles of Fortinet's CVE-2020-9294.

- I discovered a threat actor is selling a 0-day affecting a Fortinet product.

- I believe Fortinet didn't handle it properly.

What do you think?

<https://twitter.com/underthebreach/status/1255912083536969731>

Luca - April 30, 2020, 12:59 pm

Nice to see you still hustling bro. News channels still on your ass lol?

TheCyb3rAlpha - April 30, 2020, 4:14 pm

Here's what I think:

It's possible they were trying to stop the leak from happening. If Fortinet replied to you, then they had to do something about it. Even their acknowledgment would not have been good for their image in the market.

It's quite possible that the reputation loss would result in some kind of negative commotion in their upcoming projects, which could affect the balance sheet of the company resulting in a drop in stock prices, which would result in a company's devaluation. I'm no economist but these things does affect the stock market price and if the company would have acknowledged then they had to make it public. Of course, I'm assuming and I could definitely be wrong about this.

In case, they had to acknowledge the security researcher who found the 0-day or discovered it in an underground forum, it's quite obvious that they ask the researcher to sign an NDA. Maybe, (just maybe) by doing this, they'll be assured that the leak won't happen from the researcher's end. For a company whose forte is selling security products, if they found a 0-day, I don't think they'll announce it publically until it's patched.

If I was the man in charge, I would have asked you to sign the NDA and then silently asked the person about the 0-day, (maybe buy it), and then I would have asked the team to patch the vulnerability by analyzing the exploit. Once the patch is done, I would have leaked it publically (CVE) with your reference and acknowledgment with a condition to not correct the timeline of the release in public. This way, I would have scared the customers and in the next few hours, I would have released the patch.

This way I would have built a repo of 'lightning patch service' to my company's name to increase the repo, which increases the number of upcoming projects, which increases the stock price of my company and finally which makes me more money.

Again, I don't think that's the case. I just think that COULD BE the case here.