Common Types Of Vulnerability Disclosure When Working With Ethical Hackers

BY ANNA HAMMOND · MAY 24, 2021 · LAST UPDATED ON MARCH 6, 2025

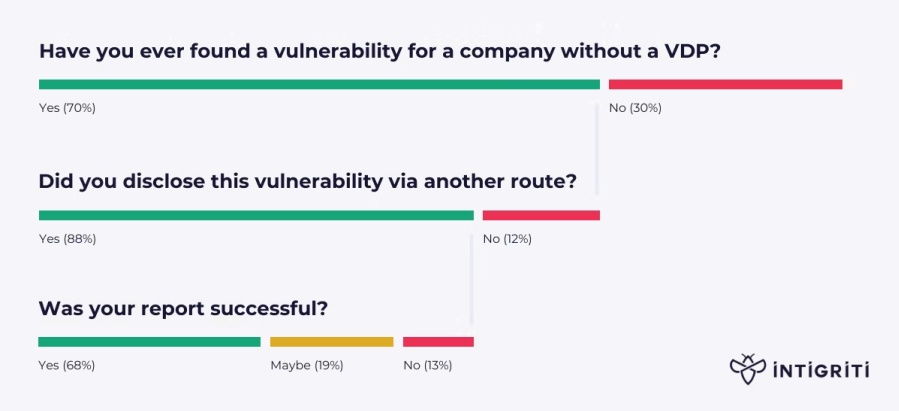
Vulnerability disclosure refers to the method whereby an ethical hacker reports a security flaw or issue to a business. In this article, we explore the three most common types of vulnerability disclosure: Private disclosure, full disclosure and responsible disclosure. We also reveal how organisations can encourage researchers to follow the method that suits them best through a bug bounty platform.

Types of vulnerability disclosure

Private disclosure

Private disclosure is exactly as its name implies — a method whereby researchers report vulnerabilities to the organisation privately. The company may disclose the security flaw to the public after a patch has been introduced. However, this decision lies with the company and *not* the researcher. In some cases, the vendor may never make the vulnerability public.

The challenge of this model is that, if the organisation forgets or doesn't respond to the researcher, they won't know whether a patch has been introduced. According to our Ethical Hackers Insights Report, this is more common than you might think; 70% of our bug bounty community have identified vulnerabilities before but found no vulnerability disclosure policy (VDP) to report them. For those that still tried to submit a report, 32% said they weren't sure whether it was successful.



Source: The Ethical Hacker Insights Report 2021 by Intigriti

Whether it's out of frustration or concern, a lack of response is the main reason researchers divert to full disclosure.

Full disclosure

Full disclosure is also known as public disclosure. This involves the researcher disclosing an organisation's security flaw to the public as quickly as possible — even if a fix hasn't been attempted yet. Doing so makes stakeholders who could be affected by the issue aware of it. It also puts pressure on the business to take urgent action to patch the security vulnerability.

Full disclosure comes with some risk, however. In making the full details (including the exploit code) available to everyone, the details are available to cybercriminals too. Knowing the possible outcome, why would a security enthusiast take this approach?

The most common reasons include:

- The researcher is unsure of another disclosure route
- They can't reach the relevant stakeholders within the business
- The business ignored or didn't respond to the vulnerability report
- The company doesn't fix the vulnerability report within a reasonable timeframe
- They wanted urgent action
- They're afraid of legal repercussions.

Many businesses prefer to avoid public disclosures because they can lead to negative press and put undue pressure on their security team.

Responsible disclosure

Responsible disclosure involves a security researcher disclosing a vulnerability publicly, but only after the business has had time to introduce a patch. Typically, the company provides a standard timeframe to remediate the bug but may ask for an extension due to complexities. In this case, the report will remain unpublic until the security team has had enough time to fix the security issue.

The benefit of a responsible disclosure method is that the security weakness is already fixed before it becomes available to the public. This reduces the opportunity for malicious actors to take advantage of the vulnerability. The challenge of this approach is that ethical hackers can become frustrated by a genuine or seeming lack of urgency to eliminate the risk. As a result, they may grow tired of waiting and revert to a full disclosure instead.

What is a vulnerability disclosure program?

A vulnerability disclosure program is the process by which a business receives vulnerability reports. A good vulnerability disclosure program will provide security researchers with clear guidance of the reporting steps in the form of a vulnerability disclosure policy (VDP).

Why do companies need a vulnerability disclosure policy?

To illustrate why a company needs a vulnerability disclosure policy, imagine this scenario. You notice your neighbour has left their car keys in the ignition of their car. As a friendly neighbour, you'd likely want to alert them to the very real opportunity that their car could be stolen. Most people would agree that the easiest way to let them know would be to call their mobile. But, say you don't have their mobile number — what now?

You could knock on their door, but what if nobody answers? You could pop a note through their post box, but will they see it in time? Maybe, you could leave a note on their windscreen, but what if someone untrustworthy sees it first? You could hunt down a social media profile and send a message via that channel, but how often do they check their messages — if at all? You see the dilemma.

Vulnerability disclosure programs help businesses avoid these issues by clearly defining a formalised way for people to report vulnerabilities to them. They also give the person making the report the knowledge that their message has been heard.

Methods for receiving vulnerability reports from researchers

Having the right structure and tools in place for vulnerability reporting is vital for a smooth collaboration with ethical hackers. Some companies choose to manage reports via email communication and spreadsheets while others point researchers towards their bug bounty program to make the report.

Vulnerability disclosure through bug bounty platforms

Bug bounty programs are well-suited to organisations that already have a mature vulnerability disclosure process and strong internal processes to remediate vulnerabilities. However, businesses with less maturity in these areas can work with a third-party vendor to set these processes up.

Thousands of ethical hackers are active on bug bounty platforms because they offer a reliable infrastructure for them to be successful. They also realise that if a company is progressive enough to create a bug bounty program, they take security seriously and welcome feedback from researchers. In other words, the company is worth the time investment.

Ready to streamline your vulnerability disclosure process through a bug bounty program? Speak to a member of the Intigriti team today to request a demo.

REQUEST A DEMO