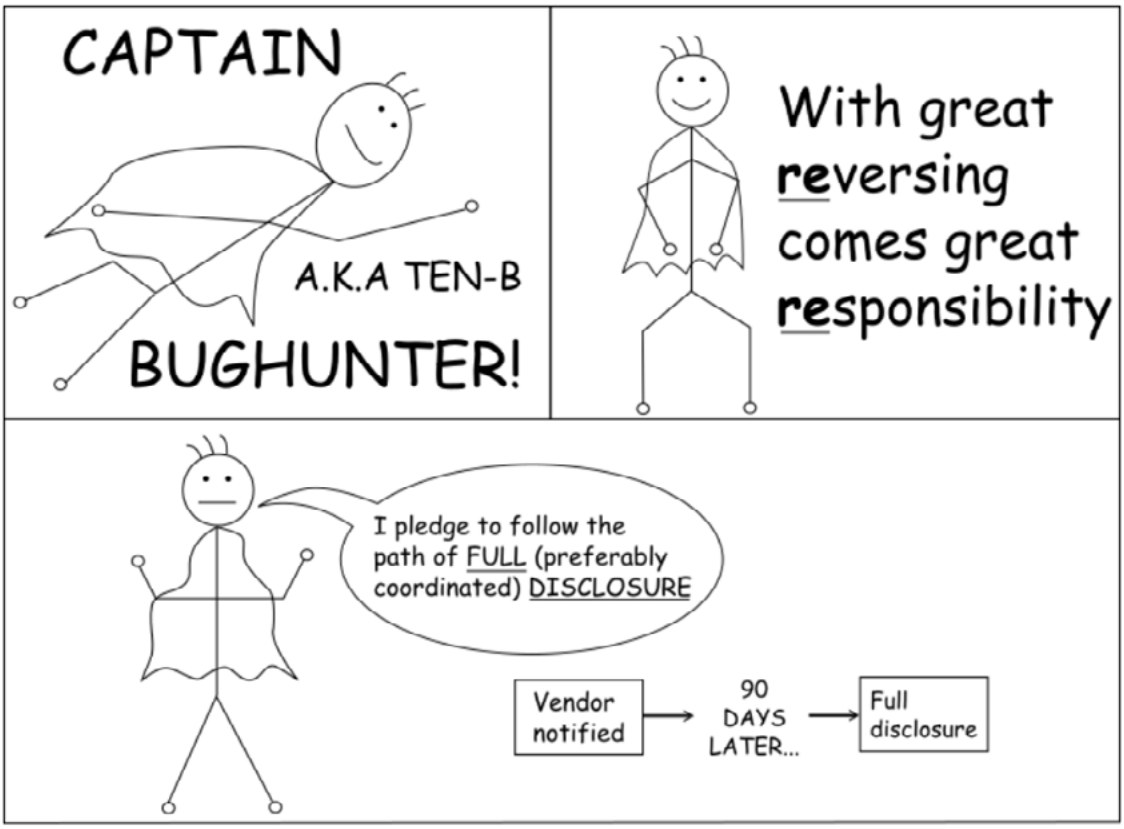
tenable

TALES OF DISCLOSURE - TEN-B ON THE MISSION

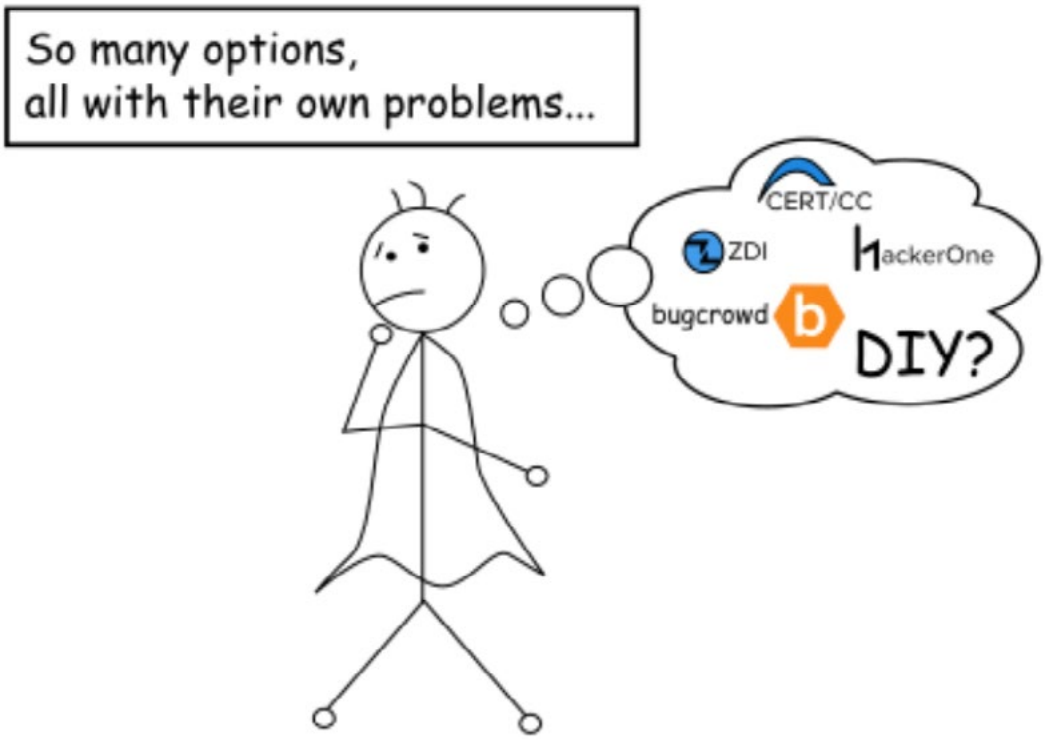
Introduction

Tenable's Zero Day Research team was established and fully staffed in late 2018. Since then, this team has disclosed hundreds of vulnerabilities to dozens of different vendors. Throughout these disclosures, this team has repeatedly confirmed something everyone in the industry already knew: Vulnerability disclosure is hard.



While there are plenty of existing resources and agencies attempting to provide some form of standardization or guidance for metrics regarding security issues, such as MITRE providing CVEs as vulnerability identifiers or First.org in establishing severity ratings like CVSS, there's no centralized authority regarding the vulnerability disclosure process itself. This leads everyone — individuals, organizations, even governments — to create their own set of processes and policies regarding such matters. Sometimes this means using an intermediary like CERT/CC; sometimes it means using a bug bounty platform such as HackerOne, ZDI or Bugcrowd; sometimes it means rolling your own process in-house; and sometimes it means doing nothing at all. As such, this makes each and every security-related bug disclosure its own unique adventure.

More often than not, these adventures are fairly uneventful since most vendors are pretty receptive to security researchers... others, well, less so. While there have been improvements over the years, the general disclosure landscape is still largely akin to the Wild West. What follows in this paper is not an in-depth look at some highly technical innovation or an analysis of the various disclosure policies in use throughout the industry. Instead, think of this paper as a lighthearted bit of self-reflection as we detail some of our more interesting disclosures over the last few years. For each scenario, we'll discuss what went right, what went wrong and what researchers and organizations can do to keep conversations regarding vulnerability disclosure moving forward in a positive direction.



Key Takeaways

- The security disclosure landscape is as crazy as it's ever been, but at least it's no longer a taboo subject for organizations to talk about.
- Tenable's industry-standard vulnerability disclosure process abides by a 90-day timeline.
- Vulnerability disclosure is a human process, and sometimes that means things get a little weird.
- It's important for researchers and vendors alike to be able to openly discuss security issues.

Tenable's Zero Day Research Team

The Team

Tenable's Zero Day Research Team exists to give back to the security community and establish Tenable as a source of expertise in areas of vulnerability discovery and disclosure. The Zero Day team's mission is to find vulnerabilities in a wide variety of products and coordinate the disclosure of these vulnerabilities with the appropriate parties.

The team releases technical write-ups on the Tenable Techblog, publishes vulnerability research via Tenable Research Advisories (TRAs), performs special projects internal to Tenable and releases tools and proof-of-concept code to the security community. Our researchers have spoken at many of the industry's largest conferences, such as Defcon, Shmoocon, and Black Hat. Additionally, our work has been featured and referenced in publications such as The New York Times, The Washington Post, WIRED and many others.

Disclosure Policy

Tenable operates on an industry-standard 90-day disclosure policy. This means that 90 days after reporting a given security flaw to a vendor, Tenable publicly releases full details of the issue(s) regardless of whether or not a fix is available. If a vendor provides a fix prior to this 90-day deadline, Tenable coordinates with the vendor to release our advisory alongside the vendor's update.

It should be noted that exceptions to this policy, while rare, are not unheard of. For example, during the height of the COVID-19 pandemic in 2020, Tenable granted multiple timeline extensions citing the "extenuating circumstances" clause of the policy for vendors that were adjusting to new or strained working conditions.

The full details of Tenable's vulnerability disclosure policy can be found here: Tenable Vulnerability Disclosure Policy

Story Time

It's important for us to self-reflect and re-evaluate our disclosure policies and procedures every now and again to make sure we're keeping in line with Tenable's values and the security industry's best practices. During these periods of reflection, there are always a few stories that pop out to us as more memorable than others. What follows are some of those stories as seen from our perspective.

Disclaimer

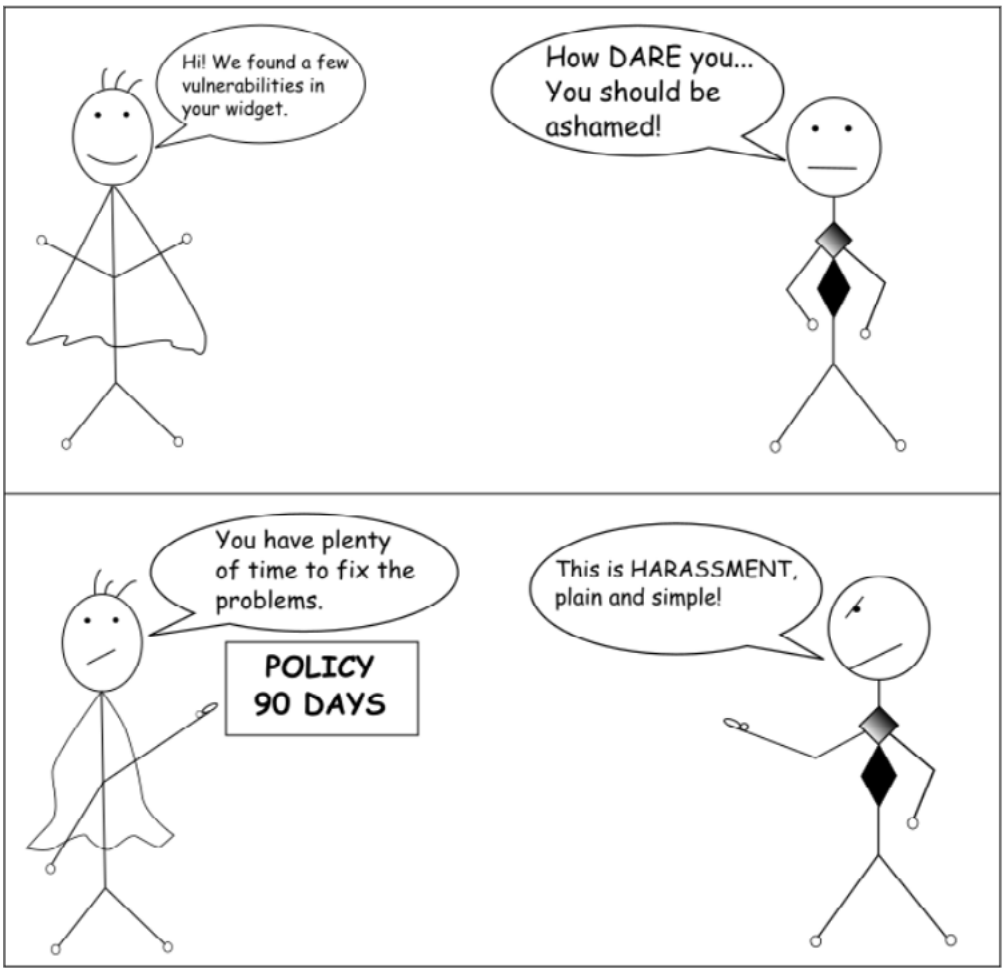
Vendors will not be explicitly named in this paper. Vulnerability disclosure is a human process and empathizing with the organizations and persons involved is necessary to move the conversation forward.

Sometimes we catch someone having a bad day. Sometimes we're the ones having a bad day. In many situations, there's probably a lot more going on behind the scenes than researchers might be aware of. In other situations, confusion may simply come down to plain old miscommunication or misunderstanding.

Feelings of Shame

When disclosing flaws in a popular medical application, the company's CEO decided to get involved. After some back and forth clarifying the issues, they stated that patches were ready and were being scheduled for release. All good so far.

Things became derailed, however, when it came time to assign CVEs to the disclosed issues. Once informed of the assignments, the CEO became actively hostile toward the researcher handling the disclosure. They expressed major disagreement with the assigned CVSS score suggestions and severity ratings. We clarified our position and gave explanations citing documentation on the CVSS standard itself. It was at this point that we received the following quote:



While a disheartening way to end a disclosure, the vulnerabilities reported were properly addressed. Unfortunately, this isn't terribly unusual. Some vendors are openly hostile toward researchers or become hostile throughout the disclosure process, such is the case with this particular disclosure. Oftentimes vendor hostility is due to some preconceived notion that security researchers are out to get them or are trying to make them look bad. Not that malicious behavior doesn't happen; it certainly does, but it's quite rare.

From a vendor's point of view, a negative reaction is somewhat understandable. It's easy for anyone to become attached to their work and take offense when its quality is questioned. This is a perfectly valid and natural reaction, but it shouldn't be the driving force behind professional communications regarding getting issues fixed.

From a researcher's perspective, it makes these conversations somewhat scary and intimidating. If a vendor is threatening legal action just because you tried to report an issue, most researchers would be hesitant to report any future issues with that vendor, especially independent researchers without the safety net of a legal department.

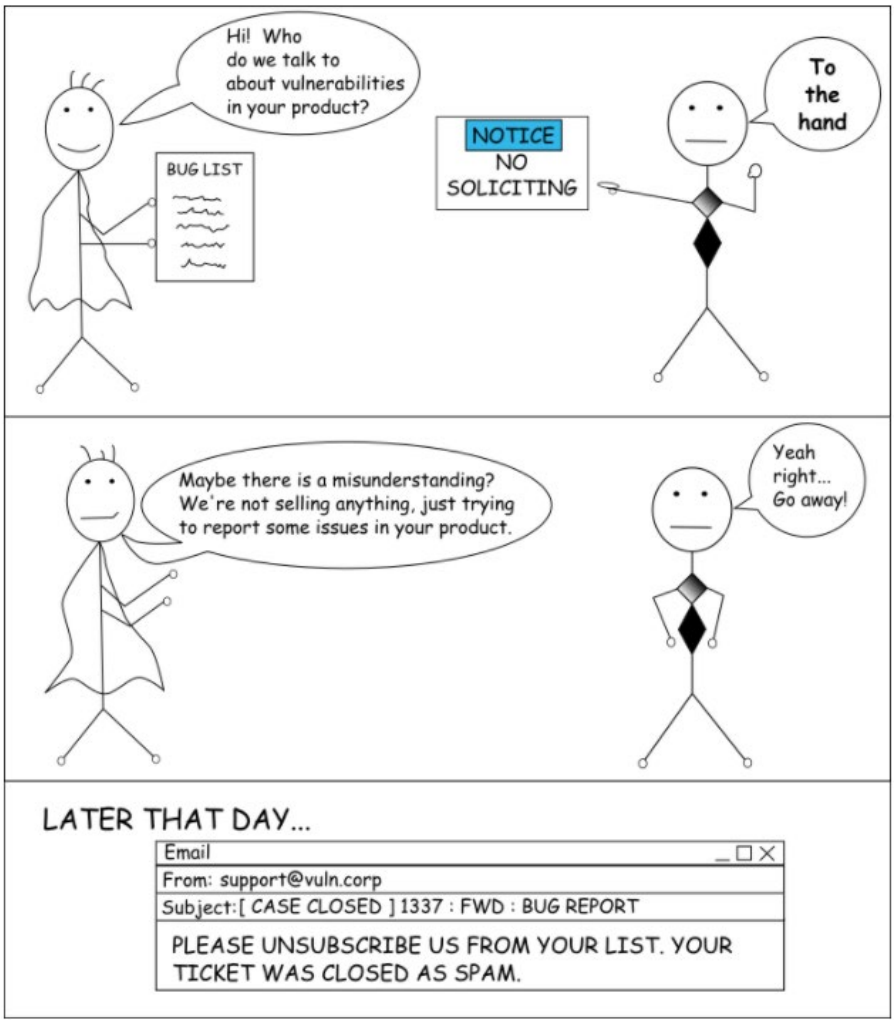
In general, it's important to put emotions aside during these conversations. Vendors need to realize that researchers aren't out to get them. Most of them just want to see issues get fixed. Additionally, researchers need to be clear about their intentions regarding a disclosure. If a researcher plans to go public with their information, that needs to be communicated to the vendor. If it appears that a vendor is becoming hostile towards a researcher, then the researcher should take a moment to remind the vendor of their intentions. If open communication does not resolve any potential conflict, Tenable encourages researchers, particularly independent researchers, to seek guidance from a third party, such as CERT/CC.

On a positive note here, the vendor in question has since been known to cite Tenable as an expert source of security-related information in some of its blog posts.

Extortion

Similar to the above, some vendors with minimal exposure to the security industry might not be too keen on responding to folks who show up claiming to have security concerns with their products. When looking at a handful of devices from a fairly niche market, we kept getting met with questions such as this:

This is interesting. How does your service work?



Essentially, each of the half-dozen companies involved had seemingly no exposure to the security industry. It took a lot of back and forth with these vendors to even find someone to disclose the discovered issues to at all. Tenable's researcher had to go so far, in one case, as to have a phone call with one of the vendors to explain that we were not trying to extort them. One vendor even asked us to send the disclosure directly to their legal department. Luckily, once everything was clearly explained and introduced, things moved forward in a fairly standard fashion.

The biggest lesson researchers can take from this interaction is not to assume that any given company, no matter size or popularity, is familiar with vulnerability disclosure. Be aware that not everyone has the same exposure to security-related topics.

For vendors, if you're selling a product and someone is trying to report flaws to you, take them seriously. Ask questions, don't just ignore them. Unfortunately, those companies lacking exposure to these processes are unlikely to ever see this paper. The best thing we can do is push for more recognition for the industry and get the general public to be more aware of vulnerability disclosures.

Conflicting Policies

Legal hiccups are never fun, but at least this one is behind us now. Once upon a time, we reported some flaws through a vendor's bug bounty program, which appeared to be the only way to contact their security team. This is not generally our preferred way of making disclosures because it introduces the potential for policy conflicts. In this case, the bug bounty program's policy stated that public disclosure of any kind was not permitted. We were very clear in our report that we would be following our own policy instead of the bug bounty's specified policy. This was mentioned multiple times throughout the disclosure process but was never acknowledged until it came time for disclosure.

As the 90-day deadline approached, we reminded the vendor and bug bounty representatives of our policy and that the issues would be published publicly. The next morning we had some wonderful legal notices waiting for us in our inboxes. Fortunately, Tenable has a long-standing history of vulnerability disclosure and a stellar reputation in the security industry. Conversations well above my pay grade occurred on both sides of the fence and our disclosure was allowed to move forward.

In the end, we wound up giving a slight extension to the vendor to appease some of its concerns and continued with disclosure. The vendor was also able to publish its advisory in tandem with our own despite the conflict. Since then, this vendor has made contact information available outside of the bug bounty program. Tenable has also amended our disclosure policy to explicitly avoid bug bounty programs unless we can receive an acknowledgment that our policy takes precedence over any other existing policy.

Definition of "Public"

Unfortunately, tempers flare from time to time on either or both sides of the fence with regards to security-related matters. In one such instance, while working through the disclosure process with a networking hardware vendor, there were disagreements regarding how the disclosure should be handled.

Chief among these disagreements was the definition of the term "public". Tenable's policy states:

"If the vendor does release a patch, security advisory, or any other information regarding the vulnerability either publicly or to any of its partners or customers prior to the 45 or 90 day timeframe, Tenable may release a Security Advisory prior to its planned disclosure date."

Essentially, revealing details of disclosed flaws to anyone outside of the disclosure process gives Tenable the go-ahead to begin informing the community of the issues involved. It isn't unusual for vendors to stop responding once they've received all the clarifications they need and post their advisories and patches without notifying us, so we periodically check the release notes of products we've submitted issues for as an indication of whether or not we can release the vulnerability details publicly. The vendor in this instance decided to release a patch to its beta platform without notifying us. It's important to note here that the vendor's beta platform is available to all of its customers and is publicly accessible.

Shortly after publication, we received a message from the vendor stating that our release of the information was irresponsible and unprofessional. Our researcher explained that our policy considers informing any party outside of the disclosure process allows us to disclose publicly. After a few frustrated exchanges from both sides, cooler heads prevailed and the matter was settled.

As mentioned, it isn't uncommon for vendors to stop responding to us once they have all the information they need and proceed to notify their customers without notifying us as well. In this scenario, Tenable could have taken a moment to give a better explanation to the vendor about why our policy is the way it is rather than giving an immediate response stating just the policy itself. Since this interaction, it has become a priority of ours to ensure that our policy is well understood if disagreements like this occur.

Silent Fixes

The trend of vendors publishing patches without notifications is our next story. When we were reporting issues for a popular chat application, the vendor repeatedly required clarification of the security flaws and how our proofs of concept worked. After a bit of back and forth, we noticed that the security issues were no longer present.

Since this was a cloud-based service, we weren't sure if the fix was intentional or not. For example, the vendor could have introduced features that broke our existing exploitation method without necessarily fixing the underlying issue. Without published release notes, we can't risk putting the community at risk without the vendor acknowledging the fix. When we requested such information, we were met with silence.

This silence lasted for the remainder of the disclosure timeline despite continued contact attempts. As the 90 days approached, we notified the vendor that we would be publishing our advisory. Lo and behold, a response! The vendor requested that we hold off as it was still validating the issues. Tenable declined this request citing our policy and communication attempts. The vendor then asked who it should credit in its own advisory. Tenable provided this information, but the credit was never published nor were the flaws ever acknowledged by the vendor.

Sometimes there just isn't much you can do beyond following through with due diligence.

Dead Silence

Building on the whole silent treatment theme going on here... sometimes we attempt to communicate with vendors that have no interest (or in this case, ability) in communicating with us.

After discovering a backdoor in a building access control platform, we made several attempts to contact the vendor through multiple methods. Receiving no response after weeks of trying, we deferred to CERT/CC, where we were also met with silence.

As the 90-day deadline came around, we published our advisory and dusted our hands of the matter hoping that someone would notice and finally get in touch with us. Fortunately, they did!

As it turned out, the contacts we were attempting to reach were correct, but were simply unmonitored due to numerous re-organizations and shifting responsibilities of teams within the vendor's organization. The flaws we originally attempted to disclose were promptly fixed and the vendor wound up establishing dedicated accounts for security researchers to contact. Since then, Tenable has received word from numerous researchers that this vendor is now far more responsive regarding security-related matters.

Incomplete Patches

Sometimes vulnerabilities aren't as easy to patch as one may think. While reporting an issue for a popular system administration utility, Tenable's researcher noticed that the vendor was fairly quick to supply a patch correcting the flaw. Upon closer inspection, it was discovered that this patch was incomplete.

This happened several more times over the course of a few weeks.

There really isn't much else to this story other than recommending stricter quality control during the development process or offering advance copies of patches to researchers so that they may provide feedback on whether or not the fix is complete.

It's a "Feature"

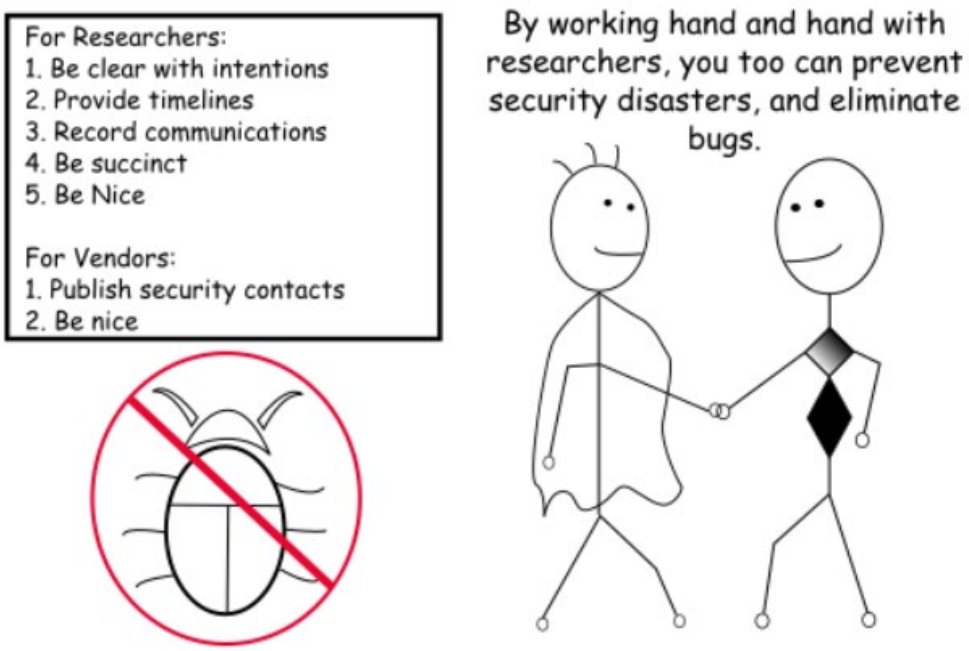
Sometimes one person's security bug is another person's feature. While analyzing installer mechanisms for a widely used operating system, Tenable discovered possible bypasses to certain security-related mitigations and discovered other areas that could harden the installer mechanisms to further attacks.

Despite referencing several vulnerable instances of the flaws, providing examples of similar flaws the vendor had issued patches for in the past and citing lapses in the vendor's documentation, Tenable was told that the issues being reported were intended as convenience features for developers.

Once again, there isn't a whole lot we can do here beyond publishing our advisories and hoping enough other folks feel the same and can assist in calling for change from the vendor.

Lessons Learned

Obviously, the above stories are quite different from one another, but there's enough in common that many of the lessons learned from them can be applied across the board. The content below summarizes these experiences in an effort to provide disclosure advice to both researchers and vendors alike.



Have Clear Intentions

This bit of advice is primarily intended for security researchers. When disclosing issues to a vendor, it is very important to be clear about your intentions from the start. If you are looking for a bug bounty, say so in your initial report. If you plan to release the information publicly or share it with others at any point, please let the vendor know. First, the vendor may surprise you and be able to give you further information and resources that benefit you in some way. Second, it's simply the polite thing to do and can help you avoid potential conflict later down the road if the person on the other end is caught off guard.

Provide Timelines

In addition to conveying your intentions during the disclosure process, it's also important to provide a timeline. Whether it's 90 days, 120 days, six months, or tomorrow, make it clear when you plan to release this information or when any other actions are going to take place.

Save Everything

Mistakes happen, it's a fact of life. In the event that disaster strikes and your actions are called into question, it's important to be able to show a record of what transpired and when. This is part of the reason Tenable prefers to keep its vulnerability disclosures in writing whenever possible. Additionally, being able to show a track record of good intentions and due diligence goes a long way to establishing credibility if future conflicts occur.

Brevity is Key

Providing detailed descriptions from both sides here is key. For researchers, this means being very specific and detailed when reporting bugs. For vendors, this means providing patch details and technical references where necessary.

It is important, however, not to be too verbose or go off on unnecessary tangents. Vulnerability disclosure reports are already lengthy documents. Adding information that isn't directly relevant is likely to cause confusion later in the process. If clarification is needed from either side, do not be afraid to ask very specific questions and provide specific answers.

Be Easy to Contact

Disclosures are difficult when you don't know how to get a hold of anyone. If a security contact isn't listed prominently on a vendor's website, Tenable is no stranger to calling up the vendor's sales team to find someone to talk to. Unfortunately, it's often the case that if the security information is difficult to find externally… it's probably difficult to figure out internally too.

Be Nice

Honestly, this is the biggest one. Security-related matters in products can be a touchy subject for some. It's important to remember that this is all a human process and the majority of folks involved are simply trying to do their jobs and what they feel is right. If tempers begin to flare, take a moment to step back and figure out what's really going on and if there's something you can do to help the situation move forward calmly.

Summing Up

People often forget that the field of tech is as much a creative endeavor as anything else we do. Developers are constantly tasked with coming up with new and innovative ways of implementing features and creating useful products. This means bugs, and sometimes, it means security bugs. It's a natural part of the process and is something that companies and individuals alike need to be mindful of. Simply having a security issue isn't a bad thing. It's how it's handled once discovered that matters.

The best way we can handle this is by owning up to it and working together to resolve issues as quickly as possible and establishing processes to quickly and effectively mitigate any risks or flaws introduced.

Author:
Jimi Sebree

Since joining in 2014, Jimi has taken on multiple roles within Tenable. He's been involved in most aspects of the plugin lifecycle at one point or another and has been responsible for the creation and maintenance of several core plugin frameworks. Prior to joining the Zero Day Research team, he was responsible for the design, creation, and launch of an internal automation initiative that serves as a primary datasource for products and workflows within Tenable. As a core member of the Zero Day Research team, Jimi discovers and publishes information regarding security-related bugs in a myriad of different products.

Visualizations by Nicholas Miles

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com

101921 V01

COPYRIGHT 2021 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, NESSUS, ALSID, INDEGY, LUMIN, ASSURE, AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. TENABLE.SC, TENABLE.OT, TENABLE.AD, EXPOSURE.AI, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.