Microsoft's Responsible Vulnerability Disclosure, The New Non-Issue

Sat Nov 10 03:00:48 MST 2001

by Jericho (security curmudgeon)

For almost a decade, a debate over the concept of **Full Disclosure** has reared its ugly head. Carried out on BBSs, newsgroups, security conferences, mail lists, parties, coffee shops and everywhere else, the Full Disclosure debate can be called "long standing" to say the least. As with everything in the computer industry before, Microsoft is doing nothing new here. Like many times before, Microsoft is re-inventing the wheel and opting for something other than round.

The debate and issues at hand are complex and go back a long way. Short of writing a small book, I can't address every issue I would like to. The following article addresses some of the bigger issues.

Branding the Enemy

In a recent essay by Scott Culp, manager of the Microsoft Security Response Center, he states that **"Information Anarchy"** must come to an end. What is the practice of "Information Anarchy" exactly? Culp answers:

> The practice that the essay was discussing was the practice of throwing exploit information out freely on the Internet without regard to how it might be used.

In short, Culp's essay argues that by publishing detailed vulnerability info and/or exploit code, it is hurting the security community and akin to "anarchy". This clever use of wording is nothing more than a scare tactic blended with a public relations campaign to help divert attention from the real problem. Economically and politically this rides the wave of preventing cyber-terrorism and suggests that anyone not with them is against them. Let me explain.

Historically, exploits/vulnerabilities start out in the hands of one person that wrote it. The author either uses it to break into machines or doesn't. After that, s/he may share it with other hackers, usually a close group of friends. Next, they begin to share the vulnerability information with more and more people for various reasons. This could be because they no longer have a use for it, are finding less vulnerable machines, or can use it to leverage newer/different exploits. After a while it leaks out to "IRC" (ie: a lot of people, not necessarily via IRC but that level of distribution). Shortly after that it often pops up on Bugtraq or another full disclosure outlet. The vulnerability information or exploit may or may not be adequate to allow others to compromise machines. Sometimes the exploits work, or end up as a variation of the original, sometimes it's crippled or proof of concept code, and sometimes it is just downright broken. The difference in the code posted to bugtraq is widespread, and the reasons are as well.

So, looking back at a one paragraph description of vulnerability progression that could easily be expanded to it's own paper, is that really information anarchy? If so, then we should label Microsoft "anarchists" and level the playing field. When Microsoft issues a patch or new program, it goes through the same exact process. It starts out at the developer, moves to the team working on a small piece of the overall product, then passed on to testers, next shared companywide, and finally released to customers or posted on the Internet.

Forget for a second what is being passed around in each example, that is

irrelevant to the term and branding here. There is a very well defined and repeated series of events, each following a fairly well defined hierarchy. To those who aren't seeing it yet.. that is not anarchy. Not by any means. Microsoft instead brands people with a different idea of vulnerability disclosure as "anarchists" in a move to brand them as outlaws or criminals.

But, **anarchy** is a great buzzword and no doubt the result of a Microsoft PR team (or buggy Word thesaurus). It conjures up really bad images and makes all the good law abiding citizens hate those exploit wielding anarchists!

Re-inventing the Wheel

As with most things labeled Microsoft, this policy for guiding the disclosure of vulnerability information is not new. In June of 2000, Rain Forest Puppy (RFP) released what he dubbed 'RFPolicy'. As originally posted:

> RFPolicy is an inititive to help establish concrete guidelines for disclosure of security problems. This was prompted due to many recent responses from vendors such as "we were never given a chance", or "there is an 'unwritten' standard of notifying the vendor X days ahead of time", etc.

> My intent is not to push this policy onto the community. Everyone can obviously do whatever they feel like. But *I* will be using this disclosure policy in all future security disclosures, and I encourage anyone wishing to use or modify it, to do so.

Later that year, RFP followed up with version 2.0 of RFPolicy. In Auguest 2001, Russ Cooper of NTBugtraq released his own ideas for responsible vulnerability disclosure.

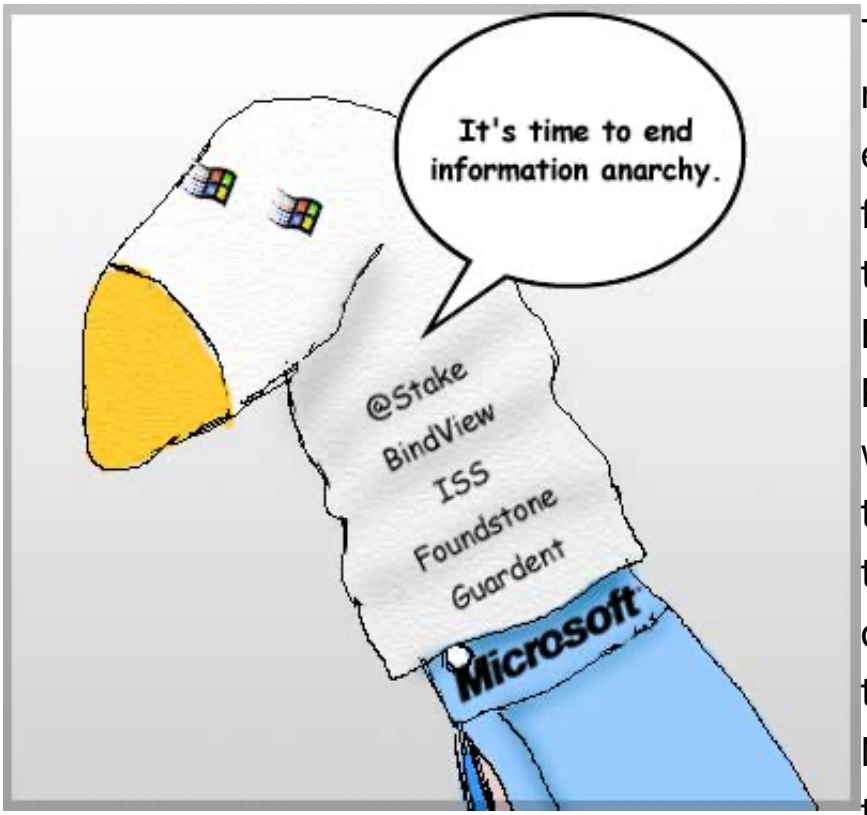
It is clear that Microsoft was not satisifed with RFP's well documented guidelines. Instead of supporting RFP's policy, they chose to rewrite most of it in their own words and tack on a 30 day "after-patch blackout" period. How original and different.

The Big Non-Issue

Since the whole idea of responsible disclosure has been done before, all of this becomes a non-issue, and certainly not newsworthy. No doubt Microsoft realized that, so they sought the help of some large security vendors to chime in, in turn making it a bigger and more newsworthy event. Scott Culp even says this whole thing is a non-issue in his original release:

> Most of the security community already follows common-sense rules that ensure that security vulnerabilities are handled appropriately.

If that is the case, then there is no reason in the world Microsoft should be pushing this new initiative like they are. Surely they don't expect the "bad guys" to follow their guidelines. If that is a given, what can really be achieved here in the way of preventing security incidents?



This entire charade is nothing more than an elaborate PR scam. The five security companies that are involved (@Stake, BindView, ISS, Foundstone, Guardent), were they not following these general rules along the lines of responsible disclosure? If so, why are they jumping on the Microsoft Bandwagon and touting this as some sort of solution? It seems to me that they would outwardly gain nothing by doing this. More interesting, Chris Wysopal of @Stake was specifically thanked for his contributions to RFPolicy, yet has become somewhat of a spokesperson for this initiative. This despite authoring and sharing the tools and vulnerability information Microsoft is now speaking out against.

One way or another this reeks of a lame PR stunt to difuse the past years of security nightmares MS has suffered due to shoddy software. To help paying customers forget about Microsoft Security Vulnerabilities that plague their systems and the news. Microsoft seems to be maniuplating these security companies today, so that they may speak out "together" in the future, even if it is contrary to the philosophy of one of the companies.

The Real Motivation

In questioning the motives behind Microsoft and the five security companies involved, i'm certainly not making friends. But for those involved in the security community have to wonder what is going on here. One security engineer at a company listed above told me his company

was **COERCED** into the meetings with Microsoft. This goes to support my analogies of Microsoft using a stick or carrot to make the security companies play ball.

The notion of Microsoft using a stick is simple. If SecurityCompanyA does not support Microsoft on this initiative, then certain negative things will happen. This could be anything from not sharing security information, revoking 'partner' status, or anything else that hurts the company. On the flip side, Microsoft may be using a carrot to motivate SecurityCompanyB into playing along. This is some incentive and could be anything from money, to contracts, or anything that helps the company.

That said, i'll take a shot in the dark on what is really going on behind the scenes here. Microsoft needs other "respected security vendors" in on this initiative to make it seem legitimate. According to one article, Steve Lipner (Microsoft's director of security assurance) said the company plans to hire an outside consultant to audit the security patch development process.

Ok, simple math anyone? One and one is adding up very quickly here. The carrot I mentioned above is right there. What is a contract like that worth in dollars? Auditing NT/2k/XP and the entire patch process, to the tune of tens of millions of lines of code. How much cash would that represent to any of those companies? Millions of dollars? Tens of millions?

Sorry, but based on what I know of the companies involved, the track record of Microsoft, the mere fact this entire things **IS** a non-issue being

blown out of proportion by Culp et all.. I can't see this as anything else. So flat out, in plain english: Microsoft is using this disclosure responsibility and information anarchy bullshit as a marketing/PR campaign and a way to solicit vendors for a sweet security audit contract.

Blame it on the "bad guys"

The solution to the disclosure problem boils down to a simple point according to Culp:

> The only thing that we are suggesting is that reasonable people should be able to agree that telling bad guys how to use those vulnerabilities to attack innocent users is wrong.

When we live in a perfect world, this will work fine. Until then we must all suffer in the reality of the security community. If labeling the bad guys was that easy, our country would have little need for law enforcement. Since the entire issue of **ethics** is subjective and based on perception often times, we live in a world of good, bad and a slew of variations that lie somewhere between. In the security industry, we label them "black hat" (the bad guy!), "white hat" (the good guy!) and "grey hat" (all those between).

So how do we define a black hat, or ensure this information doesn't end up in his or her hands? Simple, we keep the information among security professionals and not hackers and black hats, right? Wrong. At what point can you say each of those people are good and bad? It's a pipe dream to even think the world is so black and white as to allow us to conveniently 'withold' that info from 'bad guys'. This is flat out **impossible**.

In the past, exploit information has been taken from vendors (via 'hacking'). It has been shared with black hats by employees that had access to such information. It has been accidentally leaked out to the public. It has been used by employees of such companies off hours to

illegally compromise machines. How does Microsoft et all plan to deal with these cases?

Microsoft's choice of partner companies is certainly interesting. Some employees at those companies are a far cry from 'good guy' by Microsoft's definition. Some are **practicing black hat hackers**. At least one of the companies has repeatedly leaked exploit code before their own company advisories. Another company's entire research arm was labeled black/grey hat a couple years back, before they were bought and folded into the more corporate atmosphere. One employee of another company was the editor of the longest running (and most respected) technical hacker e-zine. The CEO of one company has a questionable background, and further proposes the foundation of a Vulnerability Cartel of sorts.

I personally have no problem with grey hat hackers or the background of anyone mentioned above. But if Microsoft is willing to overlook all of this and deem them all "good", while frowning upon all others releasing vulnerability information as "bad", they have amazingly reached new levels of hypocrisy.

Why This Is Doomed To Fail

Looking closer at Microsoft's initiative and comparing it to the real world, you begin to see the glaring holes in their proposal. One may draw some comparisons between Microsoft's proposal for vulnerability disclosure and seven day waits on handgun purchases. It doesn't seem to deter criminals that buy guns from places other than law abiding stores. Despite having more and more laws governing firearms, criminals still have them.

Microsoft's proposal states:

> After expiration of the grace period, members may release additional details of the vulnerability

So what happens if four days after reporting a vulnerability to Microsoft, several people see active exploitation of the same vulnerability? They report the information to Microsoft who says "We are aware of that", and then what? Does the person who just got attacked by this exploit (that isn't supposed to be out there since no one shared the information!) wait for a patch?

This entire system breaks down here. For the masses, they are now unable to do anything to protect their system short of unplugging the machine from the network. It becomes the old race condition between getting exploited and getting a working patch/fix. One thing that has been great about the past few years of vulnerability disclosure is that so many individuals and companies include temporary fixes with their information. This could be a patch to the software, a configuration change, information on tweaking a service or IDS signatures to watch for the attackt, etc. Now, the new system will eliminate that in favor of waiting for Microsoft to give you the patch info. And we know that their patches always work.

> Microsoft To Review Buggy Patch Procedures
> http://www.newsbytes.com/news/01/172041.html
>
> For the second time in recent weeks, Microsoft has released a security patch that causes some systems to crash or stop functioning properly.
>
> Unlike some instances when the company is forced to rush development of a patch, Microsoft had 10 weeks to develop the UPnP patch.
>
> Customers can receive free telephone technical assistance in recovering from the buggy patch, Microsoft said. However, instructions elsewhere at the company's Web site said customers may incur long-distance telephone charges for such calls.

With this buggy patch being released less than one month after Culp's essay, we are reminded again of what to expect from Microsoft. Do you really feel that waiting ten weeks only to receive a patch that stops your systems from functioning properly is reasonable? Do you really feel that Microsoft can and will do the right thing?

Microsoft/Culp argue:

> Supporters of information anarchy claim that publishing full details on exploiting vulnerabilities actually helps security, by giving system administrators information on how to protect their systems, demonstrating the need for them to take action, and bringing pressure on software vendors to address the vulnerabilities. These may be their intentions, but in practice information anarchy is antithetical to all three goals.

In reality, we have consistantly seen vulnerability information (often times with exploit code) be published that directly lead to a **fast and working** fix. In the middle of all this, Microsoft took **two days instead of ten weeks** to fix a serious security vulnerability in their Passport service. This vulnerability could have revealed extremely sensitive personal and financial data of millions of users.

> MS throttles research to conceal SW bugs
> http://www.theregister.co.uk/content/4/22740.html
>
> In this case, Slemko did the right thing by publishing the exploit. Microsoft immediately disabled Passport services until a workaround could be implemented.
>
> However, had MS handled it according to their new disclosure regime, all of those customers would have remained open to attack for up to a month, entirely innocent of the danger.

Conclusion

It is clear Microsoft's vulnerability disclosure initiative is nothing more than a PR stunt. They are trying to side step the onslaught of negative press surrounding their security practices. Negative press that originates because Microsoft's track record of releasing shoddy products that receive inadequate testing, no auditing, and wide distribution.

Responsible disclosure is not new. As Scott Culp said, it has been practiced by **"most"** security companies for years now. RFPolicy predates this initiative by almost two years. This is old news and a non-issue at best.

> Our reputation and our practices speak for themselves. - Scott Culp

They sure do Scott, they sure do.