SecurityFocus HOME Guest Feature: It's Time to be Responsible

It's Time to be Responsible

by Michael Morgenstern, Tom Parker and Scott Hardy
(info@globalintersec.com)

Mar 1 2002 8:19PM GMT

Over the last 12 months various computer-using groups have been intensely debating the ethics involved in disclosure of software vulnerability information, with little cross communication. These include computer security professionals, hackers, politicians, and businessmen. Even though many prominent researchers have offered their views on this subject, no consensus has been reached among them. Few of the other parties have taken any actions at all. These discussions have resulted in an even larger divide in opinion. Companies and individuals are either restricting disclosure or simply dumping information onto the internet. These parties attempt to explain their actions by claiming that their motives are justified. Some that call for restricted disclosure assert that their research is intellectual property and therefore work-product to be protected. Other motives for restriction include protection of public image and consumer opinions. Researchers who simply provide information to the general public via the internet with apparent disregard for the implications of full disclosure have different motives. To many of them, esteem with the security community (for being first at disclosing a vulnerability) is more important than the implications of their research.

At the first extreme, consider the course of information regarding the recent ssh exploit binary x2. This discovery had even the forensic consultants at the SANS institute stumped due to the lengths the author had undertaken to protect his intellectual property (http://www.incidents.org/papers/ssh_exploit.pdf). Researcher Michal

Zalewski had already published an advisory fully disclosing the details of this vulnerability. Since the information was proprietary, his advisory only detailed a theory of attack, rather than actually proving the concept. Had the source code been available, the entire community could have better shared information about this exploit. These examples abound, but still only form a tiny fraction of the big picture.

Microsoft recently bound some of the largest security firms together, furthering their monopoly by restricting these firms from releasing information about Microsoft products. Their public relations spin claims that they are looking out for the entire internet community. They assert that by stopping this information from falling into the hands of those that would use it for ill purposes until after they have had time to prepare, everyone will be safer. This essentially boils down to a big black hole – researchers working for the parties involved send information to Microsoft. Microsoft then chooses whether or not to develop a fix for the vulnerability and what timeframe is suitable for deployment (in essence whether or not to fix the problem in their next service pack). The end result – no one outside the agreement ever needs to know that the vulnerability existed.

The agreement in business terms looks perfect: Computer Security firms pay an annual fee and in exchange receive licenses, source code and other profit-creating materials from Microsoft (that financially dwarf the sum they had to pay). Additionally, they agree to disclose all Microsoft related information only to Microsoft, who then decides what should be done with that information.

By combining the largest security research businesses into an agreement covering all Microsoft products, they wrongly expect to solve many of the current issues facing the internet-using community. Their plan would create a scenario where all vulnerability information regarding Microsoft products (or at least all information discovered by companies signed into

the agreement) will now come directly, and only, from them. There are several serious problems with this situation. First, it only applies to information discovered by companies signed into the agreement. Other information will be released to the public in an uncontrolled manner – just as it has been for years. Second, by signing into such an agreement with Microsoft, security companies risk alienating themselves from their key sources that had provided them with the information in the past. This is a huge risk considering that most security firms pride themselves on having a few (and usually very few) infamous or notorious Board members or consultants in touch with the underground "scene". These connections would clearly be damaged when knowledge surfaced regarding who was profiting from the information. And losing these key connections greatly diminishes a firm's competitiveness.

The security community has had a while to try out Microsoft's new policy on disclosure. It has become clear that there are severe and fundamental problems with it. Shortly after Windows XP was released, a vulnerability was found and reported to Microsoft. It was kept secret for almost two months! Ways to get around the problem, using personal firewalls and other software, were available the entire time, but Microsoft intentionally chose not to alert the general public to them. The all-important bottom line came first.

More recently, Microsoft's .NET product range has been under intense scrutiny, with a regular stream of disclosures of vulnerability information to a public security forum – instead of to Microsoft. When unexpected vulnerabilities are released directly to the public, Microsoft has two options to address them. They can either wait until they develop a patch and leave all the systems using their software unprotected until that time. Alternatively, they can issue a work-around for the problem. In a recent disclosure, it was revealed that Outlook was susceptible to a problem whereby emails written with "Begin" as the first word would be corrupted so all remaining words would be hidden (when read in Outlook).

Microsoft's original fix was simply a recommendation not to use "Begin" as the first word. They later withdrew their advisory.

The correct answer, for Microsoft or any other vendor, is far simpler than any limited disclosure agenda, and vastly more enforceable – pay far more attention to the security aspects of software before releasing it! Hire a reasonable number of skilled security staff. And listen to what they say, even if it means that a desired feature has to be left out, or that the product ships a few days later. The current state of the legal system both in the United States and in the United Kingdom (neither of which hold software manufacturers responsible for product liability) does not excuse putting out products known to be flawed. Microsoft is clearly disregarding consumer safety and hiding behind lax legal codes. While this is possible due to their market share, it's high time consumers started reacting appropriately by boycotting insecure products and demanding fixes for those already on the market. While it would be naïve of any software firm to either claim or expect that their product is 100% secure (despite such claims by many companies) there is clearly large room for improvement. Software vendors and security communities need to rethink their current interactions and develop a new mindset toward cooperation. These partners can then work together in a responsible and productive fashion without selling out to software giants.

Some security researchers take the exact opposite approach. They publish vulnerability information on the web's security lists immediately after discovery. This approach shows lack of consideration to the implications of posting such information to public forums. Few system administrators have the extra time to instantly keep up with every posting. Compounding the problem, vendors often do not have enough time to create a fix for the problem, before an exploit becomes readily available.

As a result, many of the less talented attackers in the hacker community simply download this information, check for easy targets, and then hack

whatever unprotected computers they find. While this involves little skill, it has become a common activity in the computer underground. Compromised systems are then often used to mount denial of service attacks against other internet users, websites, and high profile targets. Clearly, this approach to disclosure also has fundamental problems.

Thankfully, for all our sake, there is an alternative to these approaches. Rather than stopping all progress and development, simply to prevent black hats from breaking into the computers of overworked administrators, security research should follow a "Responsible Disclosure" model. As is often the case, the middle ground offers benefits to everyone, from the vendors to the end-users. Such a course must enable software companies to create patches by giving them sufficient information about the problem, while also ensuring that the information does not fall into the wrong hands. For this process to become reality, several steps must occur to better communications between the relevant communities.

All parties involved in security research should present newly discovered vulnerabilities to the vendors first and allow them the opportunity to correct the issue. Some vendors may ignore such information, but in a free market that is their choice. If vendors do ignore the warnings, then releasing a public advisory is warranted. Several results should occur from this process – as computers get more secure, computer users will turn away from those companies ignoring such information. Some companies will realize the importance of this type of information and welcome it (perhaps one day even pay for it). They will choose to focus on such valuable information and will increase their business in return. This shakeout will then cause the entire system to become more secure and contribute to an ongoing development process.

A recent Global InterSec advisory (Dec 12, 2001) about glibc vulnerabilities exemplifies this situation. Immediately after discovering the

vulnerability in our lab, Global InterSec's staff contacted SuSE GmbH (the vendor who's platform was used to research this vulnerability). We gave them the opportunity to correct the problem. They agreed to work with us on correcting it – a commendable action. While this was occurring, Flavio Veloso discovered that the same bug was exploitable and contacted Redhat. Poor vendor communication lead to the disclosure of this vulnerability before SuSE, or any other vendors other than Red Hat, had time to create patches to fix the bugs. Ideally Redhat would have waited until SuSE was also prepared, but in a dog-eat-dog world, this was an acceptable outcome.

The timeline for Global InterSec's release follows: After we discovered the glibc issues, we researched the probable impact of this vulnerability and found that it had potential to do a lot of harm. We then contacted the vendor (SuSE) and stopped all related information from leaking until patches were available. Our model showed that the potential damage in this case (very similar to most discoveries) was dependent on the amount of time systems administrators would have to patch their systems before an exploit was developed and passed around in the underground. Allowing the vendor some lead time minimizes the potential impact (assuming that the vendor takes such information seriously and attempts to correct it). If they do not, then whistle blowing to the entire computer using community is appropriate. This approach increases everyone's security posture, not just those out to make a buck.

There are several solutions to this problem. As is often the case, some are easy and painless, and others require a world-changing shift in practices. Hopefully, consumers will soon recognize that the computers and the internet are no different from any other product and that they can demand accountability for their money. To hasten this process and solve the industry mess of vulnerability release practices, researchers need to follow several important practices:

1. Go to the vendors first, and allow them the opportunity to fix their code.
2. If they do nothing (such as is often the case with Microsoft) then disclose the vulnerability information (not the exploit) to an appropriate forum – something with a high readership such as BugTraq.
3. Stay out of binding agreements with companies that seek to prevent innovation and control the entire market.
4. Hold software manufacturers accountable for their products.

Similarly, consumers should:

1. Understand that software is not 100% secure and actively participate in their own personal computer security.
2. Buy programs only from vendors who fix problems, and not from those that overlook security.
3. Actively check public forums for posts of new security information and patches.

There is a clear and present danger to irresponsible behavior. The world has recently been awakened to the threat of previously unimagined acts. New discoveries of terrorist activities are occurring almost daily, and include such oddities as reports by the FBI's National Infrastructure Protection Center that members of Al Qaeda have attempted to remotely access the network schematics of U.S. utility companies' water supply, distribution, and treatment centers. It's time to take proactive steps to prevent future damage. All computer development communities (white hats, black hats, gray hats, and software developers) must come together to promote responsible disclosure.

Michael Morgenstern, Tom Parker, and Scott Hardy are Principals at Global InterSec LLC. and may be reached at info@globalintersec.com