OPINION:

# Keeping Security Issues in the Open

Contributed by Chris Davies
osOpinion.com
October 26, 2001

Send this Article Related Stories
Print this Article


**Microsoft's security manager is arguing, in effect, that security issues should be kept secret - and out of the flow of publicly available information.**

**In This Story:**



The manager of the security response center at Microsoft (Nasdaq: MSFT), Scott Culp, apparently wants to keep security issues in a box -- and out of the hands of those affected by them.

"Code Red, Lion, Sadmind, Ramen, Nimda. In the past year, computer worms with these names have attacked computer networks around the world, causing billions of dollars of damage." So begins the latest diatribe from the head of Microsoft's security response center.

Culp goes on to criticize the manner in which security professionals publish the precise details of security holes they find in software on Web sites and other public distribution media.

He proposes a culture of secrecy, where the security professional should share his knowledge only with the software retailer or development group. This, he says, will "raise the bar" for those seeking to write destructive worms and virii. Culp finishes with a call to security communities to get on the "right" side of this issue, e.g. Microsoft's side.

## Mea Culpa

It is disturbing that Culp has determined exactly what the right course of action is, without first holding any open and honest consultations with the groups affected.

It is my opinion not only is what he says untrue, it also could be harmful to the discovery and ultimate removal of any security flaws.

## Propaganda by Word

In the first paragraph of the section entitled "Arming the Enemy," Culp says that "if there hadn't been security vulnerabilities in Windows, Linux and Solaris, none of [these worms] could have been written."

The existence or not of security holes in a particular product has no effect on the ability of a programmer to write a particular combination of assembly code which exploits it. While it is true to say that the existence of the hole ensures there is a point to writing the code, its existence is not a prerequisite of writing the code to exploit it.

## Insecure about Security

Culp has a new term for the way in which security bulletin Web sites work. That term is "Information Anarchy."

He describes how this information anarchy is responsible for the recent spate of worms, because step-by-step instructions were available for the exploit of each flaw.

Whenever a piece of software is exploited by a security flaw -- missed by the programmers involved -- it's merely a race between the post-production team at the development company and the less

scrupulous members of society as to who discovered that flaw first.

The Great Race

I would suggest that what a security bulletin has done by highlighting the flaw in question is to turn an unfavorable race -- dependent largely on random chance -- into a race pitting the security team of the software development companies against the efforts of lone hackers.

If Culp is trying to suggest that this is a race that the security team cannot win, then I think he may have hired the wrong staff.

Patchy at Best

Culp also states that the only way of protecting a computer network is to apply patches. That, too, is false. The informed sysadmin may choose to protect his or her network by switching to a more secure alternative. These individuals can only make informed decisions about which product to choose if kept informed as to the relative merits of each one.

I would suggest the only reason to keep sysadmins in the dark is to keep them from switching from an insecure product to one that is relatively secure.

What of the worms that already had patches available to protect against them? Scott may be rightfully proud of Microsoft's record of patching early and patching often, but if the users do not apply these patches, of what value are they?

Out of the Box

Culp points out that many people blame the complexity of the patching process for the propagation of such worms. I on the other hand would nominate a different fault.

Microsoft prides itself on producing turnkey products, products that work "out of the box." This approach is incompatible with security concerns, as it encourages a culture of laziness whereby a small minority of admins feel they have no need to keep abreast of the current security status of their chosen product.

Shout Fire

Culp compares publishing exploit data to shouting fire in a crowded theater. Well, if there is a fire what else should one do? If one cannot reasonably expect the theater to provide smoke alarms and perhaps also a sprinkler system, why should we not warn our fellow moviegoers?

There we have the essence of what is being said. It is nothing but self-serving rhetoric to ensure that Microsoft and companies like it can save face in future. Microsoft has suffered a significant loss of prestige as a result of the recent worm attacks on IIS, and now many are calling for a complete rewrite to prevent future disasters.

As Culp says, modern software systems are unlikely to be bug-free. So, the best we can do is alert all parties involved about any bugs we find. That way, everyone can stay ahead of the game. END

Respond in the Talkback Forum

---

**Author's background:**

---

**Chris Davies** is an unrepentant nerd from the UK and has a strange addiction to jelly beans. You can reach him for feedback at c.davies@cdavies.org, although he does have a nasty habit of posting any

such feedback on his site, http://www.cdavies.org/.



## See Related Stories

Hypocrisy Taints Censure of Microsoft
(24-Oct-01)
Microsoft, Who Let the Bugs Out?
(23-Oct-01)
IT Anarchy From the Redmond Giant's POV
(19-Oct-01)