


SECURITY

MS says stop discussing hack exploits

Gives a blueprint for worms

 [John Leyden](#)

Thu 18 Oct 2001 // 13:43 UTC

Microsoft's security chief has accused the security industry of creating "information anarchy" by openly discussing exploits when security vulnerabilities come to light.

In an [essay](#), Scott Culp, manager of the Microsoft Security Response Center, said that the full disclosure approach to issues taken by the security community does a disservice to end users, and has called for a rethink.

"It's high time the security community stopped providing blueprints for building these weapons", such as Code Red, Nimda or the Ramen worm, Culp writes. "And it's high time computer users insisted that the security community live up to its obligation to protect them."

Culp readily concedes that *all* vendors have a responsibility to limit security flaws and that security vulnerabilities should be discussed but he takes issue with the "practice of deliberately publishing explicit, step-by-step instructions for exploiting security vulnerabilities, without regard for how the information may be used."

Security vulnerabilities are a fact of life with complex software so the question becomes how we deal with the issue, he states. The "information anarchy" that exists now guarantees the use of vulnerabilities by hackers and other ne'er do wells.

"The relationship between information anarchy and the recent spate of worms is undeniable," Culp said. "Every one of these worms exploited vulnerabilities for which step-by-step exploit instructions had been widely published [and] using the same techniques as were published."

Oh no, you're thinking, yet another cookie pop-up. Well, sorry, it's the law. We measure how many people read us, and ensure you see relevant ads, by storing cookies on your device. If you're cool with that, hit "Accept All Cookies". For more info and to customize your settings, hit "Customize Settings".

Customize Settings

Accept All Cookies

If portions of the security community continue to act in way that abuses free speech (he compares the action of some to "yelling 'fire' in a crowded movie house") then vendors pull back from openly addressing security vulnerabilities and find some [unstated] way of addressing customer issues. What this means (other than a knee-jerk reaction from Microsoft) we've no idea.

Culp's essay, which doesn't have much to say on how to end the threat of worms (in fact he suggests they will always exist) reopens the debate about whether information about security flaws should be controlled, or made freely available in open disclosure mailing lists (such as BugTraq).

We agree with Culp that exploit codes shouldn't be published (fewer tools in the hands of s'kiddies has to be a good thing and we're not convinced exploit codes help people test for vulnerabilities) but disagree with the suggestion that people should hold back on discussing the details of security issues. For one thing, such information can provides ways to mitigate risks before a vendor patch comes out.

The essay labels the whole security community together and fails to say that the main problem lies with people writing worm writing toolkits (such as that which created the Anna Kournikova worm) and black hat hackers writing code.

These are people Microsoft has no hope of controlling and it fails to understand the Internet if it thinks that it, or security vendors, can restrict the flow of information it takes exception to.

Microsoft is always going to be a prime target for hackers and that being so it needs to work closely with the security community when problems are brought to its attention, in fact security vendors tell us it is getting better in that regard.

Perhaps with this increased security awareness (and criticisms by heavyweights such as Gartner about IIS) Microsoft has come to see that it has much to do, hence the occasional need of those most at the front line to vent off their opinions in public.

Let's have closer co-operation between Microsoft (or Linux vendors) and security firms in the interests of end users - not a return to the bad old days when Microsoft used to claim that a particular vulnerability was purely "theoretical" @


Oh no, you're thinking, yet another cookie pop-up. Well, sorry, it's the law. We measure how many people read us, and ensure you see relevant ads, by storing cookies on your device. If you're cool with that, hit "Accept all Cookies". For more info and to customize your settings, hit "Customize Settings".

Customize Settings

Chinese researchers' claimed quantum encryption crack looks unlikely

Near-term vulnerability of RSA-2048 keys not so near, says quantum boffin Scott Aaronson


SECURITY

4 hrs | 2 

Here's how to remotely takeover a Ferrari...account, that is

Connected cars. What could possible go wrong?


SECURITY

7 hrs | 14 

Adobe will use your work to train its AI algorithms unless you opt out

Content analysis system scans data stored on its Creative Cloud services

AI + ML

13 hrs | 17 

It's time to fill those cloud security gaps

Here's how Wiz can help

SPONSORED FEATURE

Quantum entanglement discovery could enable futuristic comms tech, Nuclear physicists say

So that must be why the Russians might have hacked the DoE, right?

SCIENCE

14 hrs | 5 

Microsoft's Nadella: Tech is in for a rough two years

Slowing demand and economic pressures are a drag, but AI waits at the end of the rainbow

AI + ML

16 hrs | 9 

CES Worst in Show slams gummi gouging, money-wasting mugs, and other dubious kit

Oh no, you're thinking, yet another cookie pop-up. Well, sorry, it's the law. We measure how many people read us, and ensure you see relevant ads, by storing cookies on your device. If you're cool with that, hit "Accept all Cookies". For more info and to customize your settings, hit "Customize Settings".

[Customize Settings](#)

Criminals hit 1,800 victims across 71 countries to the tune of \$100m+

SECURITY

20 hrs | 1 

Cybercrooks are telling ChatGPT to create malicious code

Chatbot might let unskilled criminals launch attacks, if the code works


AI + ML

20 hrs | 11 

Samsung expects profit dive as demand for memory and devices continues to slow

Analysts believe company may cut back on production like Micron and SK hynix


STORAGE

21 hrs | 5 

Fancy a quick tour of DragonFly BSD 6.4?

We buzz around new version of the other-other-other FOSS-xNix-that-isn't-Linux


OSes

22 hrs | 16 

Uncle Sam OKs vaccine that protects honeybees against hive-destroying bacterium

Maybe humans could learn a thing or two about how modern medicine can prevent the spread of disease

SCIENCE

23 hrs | 18 

The Register Biting the hand that feeds IT

About Us



Our Websites



Your Privacy



Oh no, you're thinking, yet another cookie pop-up. Well, sorry, it's the law. We measure how many people read us, and ensure you see relevant ads, by storing cookies on your device. If you're cool with that, hit "Accept all Cookies". For more info and to customize your settings, hit "Customize Settings".

Customize Settings