



**Cisco IOS Worms**  
**infectionvectors.com**  
**July 2005**

**Overview**

The 2005 Black Hat conference included a controversial presentation by former Internet Security Systems (ISS) analyst Michael Lynn. This presentation covered the possibility of using flaws in the Cisco IOS (the operating system that runs Cisco routers and many of its switches) to take control of a piece of network hardware. If possible, this would be the first step to developing network worms that attack and propagate via routers and switches.

**I Left My Heart...**

The very scary scenario posited by Mr. Lynn and the ensuing media reports probably put a lump in the throats of many network and security administrators. Reports from the conference indicate that the demonstration was successful; the "enable" prompt, allowing a user to make changes and read configurations on the device was accessible after the exploit. The flaw in question, however, was one from April of this year, and had been subsequently patched. The implication, of course, is that the next vulnerability discovered will allow for the same types of attacks. Furthermore, as Mr. Lynn indicated in interviews, he fears that malware coders are already working on such an attack and plan to hit the backbone devices.

Such an attack could be devastating to the global Internet infrastructure, as well as incredibly powerful launch pads for intrusions into the majority of networks. Moreover, this could be the framework for hitting other manufacturers' routers, not just Cisco Systems'.

Mr. Lynn had discussed the possibility of such a worm in recent weeks, stating to

"It doesn't look like there are going to be any 'super-router' threats of router worms probably for the next 24 months."<sup>1</sup>

After the presentation in Las Vegas, Nevada, Mr. Lynn conceded that lawsuits would be filed against him for releasing the information. In addition, it is quite possible that ISS and Cisco could be seeking criminal charges as the router manufacturer noted that Lynn illegally reverse engineered the IOS. The information disclosed could also be considered proprietary to ISS, who sponsored at least some of the research. At this point details of Mr. Lynn's employment agreement are not publicly known.

Lynn felt the presentation was important because of the probability of attack and the costs of delaying the release of this information.

## **Forwarding**

It is very important to note that there is not an unpatched vulnerability in the IOS that allows for this type of attack currently. In addition, most of the flaws previously found in the Cisco OS required that very specific services were running on respective devices and that certain ports were accessible. That limits the exposure to a smaller percentage of boxes than every Cisco-produced device.

Cisco states that they are working on the issues with ISS. Although it is alleged that the manufacturer was “burying” the flaw, there is no indication that Cisco intended to hide the report indefinitely, only until they had developed a mitigation plan that fit the majority of its clients.

Lynn retorted that the recent theft of IOS code (in the spring of last year) indicates that time is of the essence – the only reason for such a theft is to plan an attack. That may be true, but it is not a foregone conclusion.

No matter where one comes down on “full disclosure” it cannot be denied that the recent history of vulnerability releases has been in favor of controlled notifications. The last few years have been devoid of serious “zero-day” attacks, bolstered by a vendor’s secrecy surrounding a known flaw in their products. In fact, the proof-of-concept releases soon after or prior to vendor releases have often expedited the use of exploits in malware. The Jevprox Trojan from July of 2005 was based on the pre-bulletin release of the JVIEW Profiler exploit. The debate around full-disclosure is often charged with personal opinions and sometimes paranoia over engaging giant companies like Microsoft and Cisco.

In the end, it must be conceded that delivering the details of an exploit such as Mr. Lynn’s to an audience like the Black Hat conference attendees potentially offers critical details of an attack to nefarious individuals (not that those at the conference aren’t all upstanding technology enthusiasts, but the public nature of the event means that all types of people will end up with the briefing). Allowing vendors and security groups (such as US CERT) to decide which path to take is the only means of controlling both the exploit release and mitigation release – the latter being a critical portion of the puzzle if one is to make informed disclosure choices.<sup>2</sup> Consider that for full disclosure to work as its proponents intend, there needs to be disclosure of the complete set of data – meaning that the source code to the affected applications should be available. That is not possible in today’s economy and software industry. Only vendors can create patches, their input is critical to how and when vulnerabilities should be released.

No doubt many that hear a resistance to full, unbridled release of security flaw information will argue that any other system cannot be trusted, as it is capable of being corrupted (especially by multi-billion dollar companies). That is possibly true, but there is

no incentive for such a policy. If Cisco buried the release of such an exploit, they, and all of their customers would be caught flat-footed when the attack is launched. That isn't too good for business. Moreover, the unrestricted full disclosure argument's logical extension is that virus code and kits should be publicly available as well. In the past, this has only spurred additional experimentation by those with a propensity to deliver the products that others developed. Consider the numerous Agobot variants floating about the Internet, all constructed with a publicly-available and easy-to-use source code package.

### **Discourse**

The full disclosure debate (independent of whether Mr. Lynn committed one or more crimes to release this information) will certainly not be settled as a result of this developing story. However, the results of this release should not be dismissed, as the effects may not be felt for months or years after the conference.

Cisco's Press Release Concerning the Presentation:

[http://www.cisco.com/en/US/about/security/intelligence/MySDN\\_CiscoIOS.html](http://www.cisco.com/en/US/about/security/intelligence/MySDN_CiscoIOS.html)

## References

1. <http://www.itworldcanada.com/a/ComputerWorld/6c12c0c8-c6e9-42ef-8278-1176bc9b78ee.html>
2. Granted, the CERT model has been rightfully criticized for allowing vendors to drag their feet over fixes, there are many hybrid solutions possible, especially given the recent years of security-centric policies on the part of companies like Microsoft.
3. For news coverage of this presentation and resulting fallout:  
<http://news.zdnet.co.uk/internet/security/0,39020375,39211011,00.htm>