Full Disclosure is a necessary evil

Revealing the details of security holes gives everyone a chance to close them.

Elias Levy Aug 15 2001 11:00PM PT

COMMENTARY

Lately there has been renewed debate over the practice of releasing detailed information on newly-discovered software vulnerabilities, with critics charging that 'full disclosure', as it is normally called, enables malicious users to break into systems, or to create viruses and worms.

The latest rumblings of this ages-old argument have come about as a result of the Code Red worm. It would appear some folks feel that eEye's advisory of the IIS vulnerability that was later exploited by the worm was too detailed, and, in the words of one of the critics, "was the genesis of the Code Red worm".

Before we delve into the real argument, let's get a few facts straight about the Code Red worm.

The Code Red worm is based on an earlier worm that exploited another vulnerability in Microsoft's IIS server. The vulnerability was a buffer overflow in the `.htr` ISAPI filter. No details about this vulnerability were public. Yet, someone wrote a worm to exploit the vulnerability anyway.

At the very least this demonstrates that full disclosure is not a prerequisite for black hats to develop their own exploits. At the same time, with limited disclosure of the `.htr` vulnerability, few authors of vulnerability scanners and intrusion detection systems have updated their offerings to detect the hole.

'Most criticisms of eEye are not based on fact, but are rooted in a dislike of their brash style, in-your-face advisories, and choice of hair coloring.'

Anyone that has closely analyzed the Code Red worm, and read eEye's advisory on the `.ida` ISAPI filter vulnerability, will note that the worm does not exploit the problem in the manner eEye described. The method used by the worm is distinct and more sophisticated. So it appears that while the announcement of the vulnerability triggered the release of the worm, there is no indication that the detailed information provided by eEye helped the worm's author.

One has to surmise then that Microsoft's advisory is just as likely to have triggered the worm as eEye's.

It would seem that most criticisms of eEye are not based on fact, but are rooted in a dislike of their brash style, in-your-face advisories, and choice of hair coloring.

With that out of the way lets continue.

One proposed alternative to full disclosure that's been bandied about is to create a closed group of product vendors, security companies, and security experts through which full details of the vulnerabilities can be reported and shared, while the public only gets to learn of the vulnerability's existence.

This is not very different from the old days of Zardoz and other such

mailing lists, although many of you probably have not been around online long enough to remember them. One also has to wonder if this isn't the niche that CERT was meant to fill. What exactly would be different in this new group is not clear.

One thing that is clear is how quickly people forget. Any group of the size being proposed is bound to have leaks. People that like to wear hats of more than one color are known to work for the same security companies that will be joining such an alliance. You don't need to look very far into the past for examples of vulnerabilities and exploits leaking to the underground, even when smaller groups are involved. Recall the latest Unix telnetd buffer overflow. Remember Solaris' rpc.cmsd. Think back to Microsoft's RDS vulnerability. The larger the group the worse the problem becomes.

Along these lines, we start to wonder who would be allowed to join such group. What are the qualifications? Can the security staff at corporations join? Only Fortune 100? What about Fortune 1000? CERT's Internet Security Alliance makes it easy: for $2,500 a year any black hat with a business name, P.O. box, and a web site can get advance notice of vulnerabilities before most of the general public - at least in theory. Fortunately, most of vulnerabilities become public through open sources and are available to everyone at the same time.

Its also not clear how such limited disclosure groups hope to deal with vulnerabilities in open source products, or with authors of open source security tools such as Nessus and Snort. By their very nature updates to open source products reveal the details of vulnerabilities. One must assume they will be excluded from the club.

Elias Levy is CTO of SecurityFocus, and the long-time moderator of the BUGTRAQ security mailing list. In a perfect world there would be no need

for full disclosure. But we don't live in a perfect world, and full disclosure is a necessary evil.

Discussion
[Post a comment]