Is open source the new monoculture?

devblogs.microsoft.com/oldnewthing/20040504-00

May 4, 2004

Raymond Chen

Okay I know I'm going to get into a lot of trouble for even bringing up this topic... This past weekend, Ulf Harnhammar discovered two buffer overflow and two directory traversal vulnerabilities in LHA, a library of data compression functions. Since the code for this is public, it has been copied all over the place. At least one commercial archive management program and at least one commercial mail antivirus program are vulnerable. A denial of service attack is already under way against the mail antivirus program; all you have to do is attach a malformed LHA file to a message, causing the scanner to crash when it attempts to scan the attachment. When the administrator restarts the mail server, the scanner will resume where it left off... and crash again. (Somebody with more time on their hands could craft a more clever LHA file attack that takes over the mail server itself.) The fact that the code itself was public meant that everybody didn't have to write their own LHA functions. This is a good thing. However, it also means that everybody has the same security vulnerabilities. This is a bad thing. So we have one bug that can take down large numbers of machines, even though they're all running different software.

How do you track all the versions? Is there a solution to this? Is it even a problem?

Raymond Chen

Follow