Fixing security holes in other programs

devblogs.microsoft.com/oldnewthing/20040121-00

January 21, 2004

Raymond Chen

Any crash report that involves a buffer overrun quickly escalates in priority. The last few that came my way were actually bugs in other programs that were detected by Windows. For example, there were a few programs that responded to the LVN_GETDISPINFO notification by overflowing the LVITEM.pszText buffer, writing more than LVITEM.cchTextMax characters. Another responded to IContextMenu::GetContextMenu by overflowing the pszName buffer, writing more than cchMax characters. Fortunately, in both cases, the overflow was only one character, so we were able to fix it by over-allocating the buffer by one and underreporting its size. That way, if the program overflows the buffer by one, it doesn't corrupt anything. Another one overflows one of its own stack buffers if you right-click on a file whose name is longer than MAX_PATH. (These files are legal but are hard to create or manipulate.) Not much we can do to prevent that one.

So remember folks, watch those buffer sizes and don't overflow them. Security is everybody's job. We're all in this together.

Raymond Chen

Follow