SUBJECT: Access to hidden posts on phpBB
AFFECTED SYSTEMS: All versions of phpBB (including Olympus CVS as of May 18th, 2006)
THREAT LEVEL: 6/10
REMOTE OR LOCAL: Remote
PREVENTABLE: No
WORKAROUND: Provided below

Brief Summary:

phpBB security vulnerability S05180601 gives all members information about posts originally viewable to said users but then moved to private/restricted-access forums; ranging in severity from simply being informed of replies made to that topic to being able to view the (complete) contents of such replies. This vulnerability exists in the "Watch Topic" function that allows for email notification of new replies. Upon moving a topic to a different forum, checks are not carried out to determine whether or not the user has permission to access such posts. The permission-check is only carried out once, upon the initial topic subscription, and never rechecked.

Modus Operandi:

To gain access to posts that have been moved to private/restricted-access forums, a user must use the "Watch Topic" link *before* a topic is moved. Thereafter, when comments/replies are made to that post, subscribed users will receive either notification of reply, or the complete text of the post, depending on the Administrator CP settings for email notification.

This can be automated via scripts that automatically subscribe users to all threads, or by setting the user profile settings to automatically subscribe to all threads in which the user has replied.

Analysis and Classification:

Security vulnerability S05180601 does not result in remote control of the system by unauthorized persons, nor does it allow for unrestricted access to any of the content available in restricted-access forums. At the same time, it allows for possibly highly sensitive data and information to be leaked, especially taken in the light of the fact that most topics moved from the public forums to private ones normally have some sort of disciplinary action revolving around the contents of the replies, and as such, it could be dangerous to have such information released. Based on these points, NeoSmart Technologies rates vulnerability S05180601 as having a threat level of 6/10; and recommend immediate application of the workaround mentioned below.

Workaround:

This workaround provides a generic, non code-specific solution to address the issues in this security vulnerability. This is meant to be a general guideline and to provide some sort of reference to anyone attempting to fix this vulnerability.

The vulnerability outlined in this document can be fixed by means of a workaround done by replicating the code executed at the time of initial subscription that checks for user permissions for a given post before continuing with the subscription process to the function called upon during the emailing of the notification. This is strictly a temporary workaround – the load produced running these checks may not be too heavy, but nevertheless, better and more efficient solutions do exist. This workaround is simply the easiest and least demanding fix available at the moment, and it should suffice in preventing this security vulnerability from manifesting on a given server running phpBB.