Dubious security vulnerability: Disk space consumption

devblogs.microsoft.com/oldnewthing/20160405-00

April 5, 2016

Raymond Chen

Today's dubious security vulnerability goes like this:

> The $RECYCLE.BIN directory can be used to launch a denial of service attack that is not detected by any current anti-malware software. An attacker can create a file in a user's Recycle Bin directory and write to it, making it larger than the configured Recycle Bin maximum size, and eventually consume all the space on the hard drive, rendering the drive unusable.

Um, yeah, but so?

The default security on each user's Recycle Bin folder grants access only to Administrators, System, and the owner of the Recycle Bin. Therefore, if you are a regular user, you cannot attack other users' Recycle Bins. All you can do is attack yourself.

Why pick on the Recycle Bin directory? You can "attack" the system in the exact same way by creating a file in any directory you like, and writing to it until you run out of disk quota. And if your disk quota is unlimited, then you can fill the hard drive.

In other words, a user who has permission to fill the hard drive can attack the system by filling the hard drive. If you don't like that, then don't give the user permission to fill the hard drive!

Bonus chatter: There would be an issue if creating files in the Recycle Bin allowed you to circumvent security or exceed your quota, but that doesn't appear to be what the reporter is concerned about. Disk space occupied by the Recycle Bin is still charged against your quota.

That reminds me back in my school days that one way to deal with being over quota is to mail files to yourself. The space occupied by your mailbox (or as we called it your "virtual card reader") had a separate quota from disk space, so you could use both your mailbox and your regular disk space (or as we called it, your "DASD") to store files. Of course, you didn't want to keep files in your mailbox for long, because once that went over mail quota, messages would start getting deleted automatically, oldest first. But it would buy you some time until you could get things under control.

Raymond Chen

Follow