

Partial Profiles Created on a file server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-10/msg00076.html>

- *From:* Jzodkoy@xxxxxxxxx
 - *Date:* 29 Sep 2006 14:06:57 -0700
-

A handful of partial profiles have appeared on a client's W2K3 in the "documents and settings" directory.

The profiles belong to user accounts that are NOT administrator accounts.

The profiles only have three subdirectories instead of the customary twelve subdirectories. The three directories are "Application Data", "Cookies" and "Local Settings". NTUSER.DAT, ntuser.dat.log, and ntuser.ini are also created.

It is my understanding that user profiles should only appear on a W2K3 in the "Documents and Settings" directory as a result of a user logging on from the server keyboard, or by an administrator logging in via Terminal Services (which is in admin mode).

Windows Update and the client's third party patch management software both report the server as fully patched.

- 1) Is there any legitimate way that a non-admin user could create a profile on the server?
- 2) If the profiles were created by a user using an exploit to elevate their privileges via Terminal Services, how would you manually check to see that the appropriate TS patches were actually fully installed?

Thank you

.