

Microsoft Windows Vista/2003/XP/2000 file management security issues

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-03/msg00111.html>

- *From:* 3APA3A <3APA3A@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 8 Mar 2007 22:58:37 +0300
-

This is an article I promised to publish after Windows ReadDirectoryChangesW (CVE-2007-0843) [1] issue. It should explain why you must never place secure data inside insecure directory.

Title: Microsoft Windows Vista/2003/XP/2000 file management security issues

Author: 3APA3A, <http://securityvulns.com/>

Vendor: Microsoft (and potentially another vendors)

Products: Microsoft Windows Vista/2003/XP/2000, Microsoft resource kit for Windows 2000 and different utilities.

Access Vector: Local

Type: multiple/complex (weak design, insecure file operations, etc)

Original advisory: <http://securityvulns.com/advisories/winfiles.asp>

Securityvulns.com news: <http://security.nnov.ru/news/Microsoft/Windows/files.html>

0. Intro

This article contains a set of attack scenarios to demonstrate security weakness in few very common Windows management practices. Neither of the problem explained is critical, yet combined together they should force you to review your security practices. I can't even say "vulnerabilities" because there is no something you can call "vulnerability". It's just something you believe is secure and it's not.

1.1 Problem: inability to create secured file / folder in public one.

Attack: folder hijack attack

First, it's simply impossible with standard Windows interface to create something secured in insecure folder.

Scenario 1.1:

Bob wishes to create "Bob private data" folder in "Public" folder to place few private files. "Public" has at least "Write" permissions for "User" group. Bob:

Microsoft Windows Vista/2003/XP/2000 file management security issues

I Creates "Bob private data" folder

II Sets permission for folder to only allow access to folder himself

III Copies private files into folder

Alice wants to get access to folder Bob created. She

Ia Immediately after folder is created, deletes "Bob private data" folder and creates "Bob private data" folder again (or simply takes ownership under "Bob private data" folder if permissions allow). It makes Alice folder owner.

Ila Immediately after Bob sets permissions, she grants herself