

# User downgraded from Administrator to User retains the ability to list other user's running tasks

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-11/0394.html>

---

**From:** Eitan Caspi ([eitan\\_c@012.net.il](mailto:eitan_c@012.net.il))

**Date:** 11/29/02

From: "Eitan Caspi" <[eitan\\_c@012.net.il](mailto:eitan_c@012.net.il)>

To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Date: Fri, 29 Nov 2002 08:57:26 +0200

## Summary:

Windows XP presents a new option called "Fast User Switching" (FUS). This option enables multiple users to be logged on locally to the same PC at the same time, although only one user at a time can work at the station's GUI. This option is a variant of the Terminal services (which you will be able to see in the services list).

I have found that if a user is downgraded from an administrator role to a user role, and at the time of downgrading ? the "show processes from all users" check box in the "processes" tab of the task manager application was check on for him ? this ability is retained for him (probably in its profile), although he should not have this right since he is not a member of the administrators group anymore.

I could not perform any DIRECT harmful actions at other user's processes (such as killing them). The vulnerability looks like it is mostly a disclosure of a general user's activities like: which application they are running (which can be counted as a form of surveillance and lack of privacy) and maybe (I not sure if this is true) – for how long they are logged on (by the "cpu time" value of "explorer.exe" for a user).

Maybe (I didn't try) it will be possible to use application like "kill.exe" (a windows 2000 resource kit utility that kills processes by name or PID (Process ID, as shown in task manager)) via tempting the local victim to:

1. Run a local batch / script / shortcut which uses this application
2. Open an incoming email using this utility (less possible due to security enhancements in the newer MS email clients)
3. Visit web site that will use a script or a locally directed link

This vulnerability was not tested in a windows 2000 "classic" terminal server service due to lack of domestic resources (?), but it will be interesting to know if this environment is effected as well, since it is

much more "business oriented / sensitive" than a local XP.

Affected software: Windows XP Professional with SP1

Reproduction:

(Note: Directions are referred to a system with the XP start menu style, NOT the classic start menu style)

1. Log on to windows XP as a user with administrative rights.
2. Click start -> control panel -> user accounts -> change the way the users log on or off
3. Make sure both check boxes are enabled ("use the Welcome screen" and "Use Fast User Switching") and click "Apply Options". Close the "User Accounts" form.
4. Click start -> administrative tools -> computer management
5. Open the branches: system tools -> local users and groups -> users
6. Create a new test user and place it in the local administrators group. Click "create" to enable the user.
7. Log off
8. Log on as the test user
9. Open the task manager application (ctrl+shift+esc) -> select the "processes" tab -> enable the "show processes from all users" check box -> close task manager.
10. Log off the test user
11. Log on as a user with administrative rights (but NOT as the test user!)
12. Click start -> administrative tools -> computer management
13. Open the branches: system tools -> local users and groups -> users
14. Open the test user's properties and remove it from the local administrative group, and add it to the local users group
15. Perform a "switch user" action ( by clicking start -> log off -> switch user or by clicking "windows logo keyboard button"+ L ). The user's interface is locked and the welcome screen appears.
16. Log on as the test user
17. Open the task manger -> open the "processes" tab.  
you will see all the process of other logged on users (in our case ? the user with administrative rights that was logged before and locked its interface). Note that the "show processes from all users" check box is NOT selected and even dimmed so you can't change its status.

Reproduction Cleanup:

1. Log off the test user
2. Log on back to the "already logged" administrator account
3. Click start -> administrative tools -> computer management
4. Open the branches: system tools -> local users and groups -> users
5. Select the test user and delete it.
6. Close the "computer management" application

7. Click start -> control panel -> system -> "advanced" tab -> user profiles settings -> choose the test user's profile ? click delete and confirm the deletion.

#### Exploit Programs:

There is no exploit programs necessary.

#### Workarounds:

1. Don't work in a "Fast User Switching" mode. This will force the system to have only ONE user logged on at a time, and thus ? the currently logged on user will not be able to see other user's process since there will be no other users logged on at the same time?

2. A friendlier workaround that enables you to keep the "Fast User Switching" mode and eliminate the problem:

Since this ability looks as it kept in the user's profile:

- a. As a local administrator – add the user back to the local administrators group
- b. Log on as the problem user
- c. Open "task manager" and un-check / disable the "show processes from all users" check box. Close "task manager"
- d. Log off the problem user
- e. As a local administrator – remove the user from the local administrators group

This will reset things back to normal.

#### Vendor Notification:

Microsoft was alerted about this.

I think that attaching their response will give a good idea of their concept:

"My understanding is that FUS (Fast User Switching) is a consumer oriented feature – <http://www.microsoft.com/windowsxp/home/evaluation/overviews/sharing.asp> .

It's only available in Windows XP Home, or Pro when explicitly enabled AND when in a workgroup only. As such it's not a corporate focused feature. Since it is aimed at the home space, the thread profile is different – FUS is aimed at making it easy for multiple users to share the same machine whilst maintaining their own settings. It's focus is on this separation of settings to provide personalization, it is not explicitly designed to provide complete security separation of users. It does not make any promises about explicitly keeping sessions secure from each other.

The classic usage scenario for FUS is in the home, where several members of the same family share the same computer. Using FUS, different individuals can maintain separate e-mail accounts, Instant Messenger profiles etc without interfering with each other's settings. This of

course means that each individual has access to the computer, in which case, the 3rd Immutable law of security applies:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp> .

However, given the consumer oriented usage scenario for FUS, it is likely that there is a very high degree of trust between each user, as they will be part of the same household etc.

Whilst the scenarios you describe below are of course technically correct, they are unlikely. They suggest that one member of the household may decide to hack another, or deny service to another. Specifically, let's look at the denial of service scenario, where one user would enumerate the processes of the other and then craft an e-mail that called "kill.exe" to kill the other user's processes. There are a number of flaws here. If the users are using Outlook Express, then OE 6.0 is the default on XP, which blocks executable attachments. If the users are using the full Outlook client, then there is a high probability that it is one of the later versions of Outlook, that again block attachments.

Secondly, under the default FUS settings, no passwords are set on the accounts, so one user can switch into another user's session. Again this is because the primary objective of FUS is user personalization, not security separation. Thirdly, if the user has the ability to logon, then they by default will have the ability to shut the machine down (even as a limited user). This is just as effective a denial of service than having to enumerate PID's, craft e-mails etc, or altering the paths to shortcuts.

Ultimately, with FUS, the 10 Immutable laws of security apply – if I have physical access to the machine, I can do what I want. Given however the consumer oriented usage of FUS, the degree of trust that is likely between users on the same FUS enabled machine, and the fact that the primary purpose of FUS is user separation for personalization reasons and not security reasons, I think the threat rating for this style of attack is very low.

Thanks for taking the time to bring this to us"

Just one note by me: They did not mention a possibility of using FUS in a business to share a PC resource among shift workers and / or using it as a shared internet station.

Credit:

Eitan Caspi

Israel

Email: [eitancaspi@yahoo.com](mailto:eitancaspi@yahoo.com)