

# Windows XP security concerns

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-12/0217.html>

---

**From:** Tomasz Polus ([Tomasz.Polus@bsi.net.pl](mailto:Tomasz.Polus@bsi.net.pl))

**Date:** 12/20/01

Date: Thu, 20 Dec 2001 09:52:15 +0100  
From: "Tomasz Polus" <[Tomasz.Polus@bsi.net.pl](mailto:Tomasz.Polus@bsi.net.pl)>  
To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Hello bugtraq subscribers,

Below is a description of three security problems with Windows XP Professional, which we think are bugs – not features. We are actually writing a book about Windows XP security and need to clarify these concerns. Please express your opinions and let us know if you find these problems important to Windows XP security.

System affected: Windows XP Professional in a workgroup.

## I. Problem with account locking due to fast user switching

Fast user switching is a new Windows XP feature, which allows simultaneous logging on of more than one user. It is based on Terminal Services technology and runs unique user sessions that enable each user's data to be entirely separated. Fast User Switching is enabled by default on a stand-alone or workgroup-connected computer. It is not available in domains.

While extensively using this new feature, we found that it locks out accounts on our machine.

Please try this on your Windows XP computers:

1. Set the account lockout threshold to 3 attempts.
2. Create 10 user accounts with user level privileges (User1 – User10).
3. Logon using User1 account.
4. Using fast user switching, logon using User2 account.
5. Use fast switching to change from User1 to User2 3 times.
6. Attempt to logon using User3 account.

At this point, every account on the machine would be locked out (except Administrator account of course).

Security Log would now show logon failure (ID529) and account locked

## SecurityFocus Bugtraq: Windows XP security concerns

(ID539)

entries. Please see attached TXT file with event log entries.

We have also found, that there is no need to switch between \_two\_ users.

Even switching between \_one\_ user (logging on and logging off using fast user switching) results in all accounts being locked out.

We notified Microsoft on December the 5th, 2001 and received the following reply from Microsoft Security Response Center:

From: Microsoft Security Response Center [mailto:[secure@microsoft.com](mailto:secure@microsoft.com)]

Sent: Wednesday, December 12, 2001 10:54 PM

To: Tomasz Polus

Cc: Microsoft Security Response Center

Subject: RE: Fast User Switching blocks user accounts [cb]

[...] "Fast User Switching is a feature that's designed primarily for home users.

One thing that Fast User Switching does is to check local accounts for blank passwords to determine if a prompt should be provided for a particular user or not.

Users who have elected to maintain blank passwords are not shown the prompt

for their account when they switch accounts. Because of this, if account lockouts

are enabled in conjunction with Fast User Switching, it is possible for this

feature to inadvertently lockout accounts.

If you want to enable the account lockout feature, it's recommended that you

not use the Fast User Switching feature.

I hope this is helpful in clarifying what you are seeing.

Please let us know if you have any questions or concerns." [...]

I would like to point out they didn't write that only accounts with blank passwords

are locked out – which is actually right. For all of our test accounts passwords has \_been\_ set.

This problem does not affect accounts with blank passwords.

As you can see, Microsoft admitted this to be a problem and recommended

not to use fast user switching in conjunction with Account Lockout.

We see this as a significant limitation on the new feature, and/or a forced downgrading of security settings.

II. Problem with reset password disk

## SecurityFocus Bugtraq: Windows XP security concerns

Windows XP introduced a new feature – "Password Reset Disk", which can be used to recover user account and personalized computer settings if a user forgets his password.

The problem is that in certain conditions (Minimum password age  $\leq 0$ ) user may not be able to reset his password using above mentioned disk and the only solution is the reset password feature available to the Administrator.

First, make sure the "Minimum password age" policy is set to a value other than 0.

Now, supposing the user forgets his password before it's age expires, he will not be able to reset it with the disk until the password expires.

What's more, changing password by an Administrator using MMC or control panel

(in other words – GUI) leads to user data loss (i.e. EFS files) because of private key loss.

The only solution seems to be "net user" command issued by an administrator.

### III. Remote Desktop sends recently used username in plaintext

This problem was first detected by Szymon Nowak – we made the tests and drew the final conclusions.

Remote Desktop client remembers account name which has been used recently

to establish RD session with another machine.

When sniffing the network, Szymon found that RD client has send login to the

other computer in plain text. We clarified that what was actually sent is not

a user account name on the destination machine, but username which has been used

recently to logon with RD client.

However, assuming that the logon is made to the same computer as recently,

RD client sends in clear text user account name present on the destination

computer. In some cases, this can pose a big security risk. For example,

if RD client is used by users connecting to a terminal server, the attacker can sniff all the TS user accounts.

We're very interested in your opinions about all these problems.

Please try this at your machines and let us know if these are common,

## SecurityFocus Bugtraq: Windows XP security concerns

so we could find versions affected.

Regards,

--

Tomasz Polus

[tpolus@bsi.net.pl](mailto:tpolus@bsi.net.pl)

BSI Sp. z o.o. <<http://www.bsi.net.pl>>

---

- text/plain attachment: [acclockout.txt](#)
- 

- ***Previous message:*** [Jing Shen: "IE5 \(SP1\) crash the X server on Solaris2.6 chinese edition"](#)
- ***Next in thread:*** [Geoff Sweet: "RE: Windows XP security concerns"](#)
- ***Reply:*** [Geoff Sweet: "RE: Windows XP security concerns"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)