

[NT] Windows XP Security Concerns (Fast Switch, Password Reset, Remote Desktop)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0081.html>

From: support@securiteam.com

Date: 12/20/01

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 20 Dec 2001 08:45:11 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Windows XP Security Concerns (Fast Switch, Password Reset, Remote Desktop)

SUMMARY

Below is a description of three security problems with Windows XP Professional that should be considered as security bugs.

DETAILS

Vulnerable systems:

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.

Example:

While extensively using this new feature, a possible denial-of-service bug has been found that locks out accounts on the machine. To recreate, do the following:

Securiteam: [NT] Windows XP Security Concerns (Fast Switch, Password Reset, Remote Desktop)

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 (ID539) entries. It was also noted 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.

Microsoft was notified on December 5, 2001 and the following response was received:

From: Microsoft Security Response Center [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 is 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." [...]

As you can see, Microsoft admitted this to be a problem and recommended not to use fast user switching in conjunction with Account Lockout. This as a significant limitation on the new feature, and/or a forced downgrading of security settings.

2. Problem with reset password disk

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

Securiteam: [NT] Windows XP Security Concerns (Fast Switch, Password Reset, Remote Desktop)

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.

3. Remote Desktop sends recently used username in plaintext

Remote Desktop client remembers account name that has been used recently to establish RD session with another machine. When sniffing the network, it was discovered that RD client has send login to the other computer in plain text. It was further 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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:Tomasz_Polus@BSI.NET.PL>
Tomasz Polus.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] Trust Issues with RH and Debian Package Managers"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)