

# [EC-SA-01.2003] Windows XP "welcome screen" exposes the names of all the members of the local administrators group

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-03/0130.html>

---

**From:** Eitan Caspi ([eitancaspi@yahoo.com](mailto:eitancaspi@yahoo.com))

**Date:** 03/07/03

From: "Eitan Caspi" <[eitancaspi@yahoo.com](mailto:eitancaspi@yahoo.com)>

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

Date: Fri, 7 Mar 2003 23:46:35 +0200

\*\*\*\*\*  
\* \*  
\* Eitan Caspi - Security Advisory - 01.2003 \*  
\* \*  
\*\*\*\*\*

Suggested risk level: Low

Type of risk: Information disclosure

Affected software: Microsoft Windows XP with SP1

Local / Remote exploit: Local only

Summary:

Windows XP has an option of replacing the regular NT / Windows 2000 logon screen with what is called "Welcome Screen".

The "Welcome Screen" lists the full names of ALL the available LOCAL users registered in the local machine after a regular boot.

The person using the machine locally only needs to choose the desired name and simply fill in the correct password.

This option can be enabled only when the machine is part of a "Workgroup" network model (and it can NOT be enabled when it is a part of a Domain / Active Directory infrastructure).

When booting the machine using "safe mode" (description and usage can be found in <http://support.microsoft.com/default.aspx?scid=kb;en-us;315222> ("A Description of the Safe Mode Boot Options in Windows XP"), the welcome screen is loading with a different list of names: The list is made ONLY from ALL the members of the local "Administrators" group

(including the original administrator account, even if it was renamed).

Side notes:

1. Although it may look obvious due to the nature of the "welcome screen" (which is "anti security"), still, MS is not stating the following in a formal article (as far as my current knowledge): Using the "welcome screen" actually disables / ignores the security options (in the "Local Security Settings" XP application) of:

A. "Interactive logon: Do not display last user name" (On the one hand it is really not displaying the name of the last user who logged in as the only name, but on the other hand it is NOT displaying an empty field but rather allows to probe ALL the possible local users.

This option applies if you decide to use the normal logon screen after the "welcome screen" was loaded (see the note in the following paragraphs).

B. "Interactive logon: Do not require CTRL+ALT+DEL", if Disabled = CTRL+ALT+DEL is required.

2. If the only user in the local "Administrators" group is the original administrator account (regardless if its name was changed / renamed, the reference is to the same user "security identifier" (known as SID), the one ending with 500) – then this name is listed along with all the other names in the welcome screen.

If there is at least one more user as a member in the local "Administrators" group, BESIDE the original Administrator account – then the "welcome screen" omits the original Administrator from the list of names in the "welcome screen" (the one displayed in the NORMAL logon, not in "safe mode").

I guess this behavior is in place to hide at least one "administrator" account from other users and prevent local users from trying to guess the password of this account, but on the other hand – this behavior can help spotting the "Administrator" account (The one that is suddenly "gone"), and as for the main note above – "safe mode" shows it all...

3. You can still logon to "Safe Mode" (even if the "welcome screen" is used) using ANY local account by holding down the left "Ctrl" and "Alt" and at the same time pressing twice the "Delete" key -> the normal logon screen will replace the welcome screen and will enable to perform a logon using any valid local account (from any local security group, as long as the account has the right to perform a local logon).

This is opposing to what MS is stating in article 292742 (<http://support.microsoft.com/default.aspx?scid=kb:en-us:292742> "Users Are Missing from Welcome Screen in Safe Mode") -> "Users with Standard or Limited account types do not have access to start in Safe mode." This use of the regular logon screen is possible also after the "welcome screen" is loaded when performing a normal boot (i.e. not in "safe

mode").

4. Any users AUTHENTICATED after a local login procedure (regardless of its security group membership) – can open the "Computer Management" application and see the members of ALL the local groups.

I must say I can't see the reasoning for this logic – There must be some kind of hierarchy so higher accounts can review lower accounts and the opposite will NOT be possible.

Also, I guess a group can be an object that can accept security permissions and not be open to all the local authenticated users for viewing.

Possible Abuses:

Any local and un-authenticated malicious user(s) can learn of the names of all the local accounts with administrative privileges, and so they will know to focus their password guessing efforts on the most privileged accounts.

Since in small LANs that don't use any central active directory / domain, the model used is "workgroup" – usually the same name (and password...) is given to the local administrator account (be it the default / original "Administrator" account or a specially created account) in all the participating stations, in order to simplify network management – and so it takes only one station to expose the administrator(s) account(s) for all the other stations in the LAN.

Exploit Code:

No code is needed.

Direct solution:

No direct solution at this time.

Workaround:

Avoid using the welcome screen and use only the normal logon screen.

Vendor Notification:

According to MS KB article 292742

( <http://support.microsoft.com/default.aspx?scid=kb:en-us:292742> – "Users Are Missing from Welcome Screen in Safe Mode" )

it looks like MS is aware of this behavior, but it is referring only to the functional side and not to the security perspective.

Official vendor response:

Due to bad past experience with MS, regarding its willingness to post a security bulleting and a binary fix within a reasonable time frame, I have decided to form my own policy (which will be activated towards any vendor in the future) – a policy that will limit the vendor's "worry

free" time frame and force it to act seriously towards creating a solution and notify the public – all within a limited time frame.

MS received this advisory as encrypted text with the following un-encrypted text. The company declined my policy, so it was sent to bugtraq without being reviewed by the company, and thus there is no official response by MS.

The email sent to MS:

"Hello,

My name is Eitan Caspi, from Israel.

I'm sending this email to your company since I believe I found a security problem with one or several of your products.

I will be happy to cooperate with you in this matter and to conduct an efficient discussion to reach a solution.

I am attaching my PGP public key so we can exchange email in a secure way.

Since I wish to keep a balance between giving a chance to the vendor to fix the problem as soon as possible and the public's right to know about the security problem with the product they use – I have established the following policy.

If, for any reason, you decline this policy (as a whole any part of it) – I ask you NOT to decrypt the attached encrypted notification and let me know of your decline as soon as possible and I will act based on your reasoning for decline.

Of course, there is always the option for you, as the vendor, to decline this issue(s) as security vulnerabilities from the beginning – and if this is the case, please let me know of this as soon as possible.

The Policy:

1. First, I notify the vendor of the problem
2. The notification is also sent as a copy to Mr. Dave Ahmad ( [da@securityfocus.com](mailto:da@securityfocus.com) ), the editor of the BugTraq security mailing list. This is done to make sure the vendor will handle this issue seriously and to stamp this report with a "proof of originality". Mr. Ahmad has agreed to take the role of "Advocate of honor" and he obligated not to make any use of this notification nor he will reveal it to anyone but himself – until a publication from the vendor about the problem is published or by the end of the waiting period (following), after accepting my approval.
3. I grant the vendor a time frame of 30 CALENDAR days ( pay attention:

Focus Bugtraq: [EC-SA-01.2003] Windows XP "welcome screen" exposes the names of all the members of the local admin

NOT business days!) to publish a public fix or a fully detailed advisory of the problem that will also include intermediate solutions for the problem, until a final fix will be released.

Any vendor publication will include a proper and dignified acknowledgment to my help with this issue ( using the details of: Eitan Caspi ( [eitancaspi@yahoo.com](mailto:eitancaspi@yahoo.com) ) ).

The "waiting period" time frame is starting one day following the day of this email delivery.

This notification delivery date:

The first date of the "waiting period":

The last date of the "waiting period":

Date of delivery to the BugTraq mailing list:

4. If the vendor fails to response to me at all within 3 days of the first email delivery and / or to publicize at least one of the above mentioned publications types until one day after the last date of the "waiting period" – this notification report will be delivered to the BugTraq mailing list for a fully public distribution that will be delivered to all the mailing list subscribers and will be published on BugTraq web site.

End of Policy.

I believe this policy is balanced and fair for all sides, and I hope you will accept it.

Regards,

Eitan Caspi ( [eitancaspi@yahoo.com](mailto:eitancaspi@yahoo.com) )  
Israel"

Credit:

Eitan Caspi

Israel

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

Past Security Notes:

1.

<http://online.securityfocus.com/bid/4053>

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-003.asp>

<http://support.microsoft.com/default.aspx?scid=KB:en-us;315085&>

2.

<http://online.securityfocus.com/bid/5972>

[EC-SA-01.2003] Windows XP "welcome screen" exposes the names of all the members of the local admin

Focus Bugtraq: [EC-SA-01.2003] Windows XP "welcome screen" exposes the names of all the members of the local admin

<http://online.securityfocus.com/archive/1/295341>

<http://support.microsoft.com/default.aspx?scid=kb;en-us:Q329350>

3.

<http://online.securityfocus.com/bid/6280>

4.

<http://online.securityfocus.com/bid/6736>

<http://online.securityfocus.com/archive/1/309442>

Articles:

You can also find articles I have written in

<http://www.themarket.com/eng/archive/one.jhtml>

(filters: Author = Eitan Caspi (second name set), From (year) = 1999)