

Re: Vulnerability in IBM Windows XP: default hidden Administrator account allows local Administrator access

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-09/0642.html>

From: Harrison Gladden (linuxguru80_at_yahoo.com)

Date: 09/16/04

Date: Thu, 16 Sep 2004 08:24:38 -0700 (PDT)

To: Michael Scheidell <scheidell@secnap.net>, bugtraq@securityfocus.com, vulnwatch@vulnwatch.org,

This is common in most Pre-Installed Windows System. More so systems with XP HOME edition installed. From what i've seen most of the systems with XP Pro (and media center) installed give you an option for setting a password on the Administrator account.

~Harrison

----- Michael Scheidell <scheidell@secnap.net> wrote:

- > *Vulnerability in IBM Windows XP default hidden*
- > *Administrator account allows local Administrator*
- > *access*
- > *Systems: IBM Workstations, Laptops, etc.*
- > *Vulnerable: IBM Systems with preinstalled Microsoft*
- > *Windows XP Professional RTM and SP1*
- > *Not Vulnerable: IBM Systems without Windows XP*
- > *Professional*
- > *Severity: High*
- > *Category: Unauthorized Administrator Access*
- > *Classification: Default Authentication*
- > *BugTraq-ID: TBA*
- > *CVE-Number: CAN-1999-0504*
- > *Remote Exploit: No*
- > *Local Exploit: Yes*
- > *Vendor URL: www.ibm.com*
- > *Author: Jason Lash, SECNAP Network Security*
- > *Internal Release date: August 6, 2004*
- > *Notifications: August 6, 2004: secure@ibm.com,*
- > *security@ibm.com, cert@ibm.com, askibm@vnet.ibm.com,*
- > *support@ibm.com, askibm@vnet.ibm.com,*
- > *August 7, 2004: security-alert@austin.ibm.com,*
- > *cert@us.ibm.com*
- > *Vendor Response: August 13, 2004*

Re: Vulnerability in IBM Windows XP: default hidden Administrator account allows local Administrator access

- > *Public Release date: September 15, 2004*
- >
- > *Discussion:*
- > -----
- > *From www.ibm.com*
- > *Innovation for Business Advantage: IBM helps you*
- > *become more competitive and on demand by delivering*
- > *products that offer industry-leading capabilities,*
- > *improve productivity and reduce the total cost of*
- > *owning a PC. No other vendor provides as wide a*
- > *range of PC products, technologies and software to*
- > *support on demand businesses than IBM.*
- >
- > *Security: As information technology increases in*
- > *importance, so do the number of threats directed*
- > *against it; a comprehensive security strategy is*
- > *essential to protect vital data and to ensure*
- > *continuity of operations. IBM security solutions*
- > *will help protect your system and business from*
- > *network infiltration, data destruction, information*
- > *theft and unauthorized surveillance.*
- >
- > *Problem:*
- > -----
- > *IBM OEM XP and XP SP1 contain a default hidden*
- > *administrator account. Use of this account will*
- > *allow anyone with physical access to the computer to*
- > *fully control the computer, add spyware, keystroke*
- > *loggers, password stealing software and read all*
- > *files, including temp files, local files, documents,*
- > *and any email that has been stored locally. IBM*
- > *does not inform the installer of this account, does*
- > *not give them the option of putting a password on*
- > *this account, and if a savvy installer FINDS the*
- > *function to change the password for the*
- > *Administrator account, they are warned that they*
- > *could lose data. Security best practices REQUIRE a*
- > *password on all administrative (and root) accounts.*
- >
- > *Because IBM marketing directly targets large*
- > *publicly traded businesses, government agencies, and*
- > *research organizations, these systems are used in*
- > *regulated industries. Healthcare organizations must*
- > *be HIPAA compliant; financial institutions must*
- > *follow GLBA regulations; publicly traded firms are*
- > *required to adhere to the Sarbanes-Oxley Act;*
- > *federally funded educational organizations are*
- > *regulated by FERPA, and government agencies must*
- > *comply with FISMA regulations. With such*
- > *organizations comprising a major portion of IBM's*
- > *market share, it would be advantageous to ensure*

- > *that products incorporated into IBM systems would*
- > *help achieve compliance with such regulations.*
- >
- > *OEM Version of Windows XP Professional released by*
- > *Dell, HP and others have not shown similar*
- > *characteristics and has only been observed in IBM*
- > *OEM installations.*
- >
- > *This may not be the first report of this behavior.*
- > *If others have reported on this issue before, please*
- > *let us know: however, we searched the CVE database*
- > *and only found a distantly related problem dating*
- > *back to 1999 where there is a warning against*
- > *default, missing or weak administrator passwords.*
- >
- > *The Common Vulnerabilities and Exposures (CVE)*
- > *project has assigned the name CAN-1999-0504*
- >
- > <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0504> to
- > *this issue. This is a candidate for inclusion in the*
- > *CVE list (<http://cve.mitre.org>), which*
- > *standardizes names for security problems.*
- >
- > *A retail setup implementation of Microsoft Windows*
- > *XP Professional Edition, "Out-of-Box Experience"*
- > *(OOBE), requires that the installer be given the*
- > *option to add an Administrator account. During the*
- > *installation, the XP Installer states : "You must*
- > *provide a name and an Administrator password for*
- > *your computer. Setup creates a user account called*
- > *Administrator. You use this account when you need*
- > *full access to your computer." While setup will not*
- > *require that a password actually be entered, it does*
- > *stress that one SHOULD be entered. Additionally, the*
- > *user is prompted to create a regular user account*
- > *for general use.*
- >
- > *In contrast, the IBM setup implementation of*
- > *Microsoft Windows XP Professional Edition does not*
- > *include such steps. The existence of an*
- > *administrator account is never mentioned. Instead,*
- > *the setup asks: "Who will use this computer? Type*
- > *the name of each person who will use this computer.*
- > *Windows will create a separate user account for each*
- > *person so you can personalize the way you want*
- > *Windows to organize and display information, protect*
- > *your files and computer settings, and customize the*
- > *desktop. These names will appear on the Welcome*
- > *screen in alphabetical order. When you start*
- > *Windows, simply click your name on the Welcome*
- > *screen to begin. If you want to set passwords and*

- > *limit permissions for each user, or add more user*
- > *accounts after you finish setting up Windows, just*
- > *click CONTROL PANEL in the START menu, and then*
- > *click USER ACCOUNTS." By default, none of the*
- > *accounts added in this step have passwords. Nor is*
- > *there an option to set passwords during the install.*
- > *While this is not unique to the IBM install, it is a*
- > *known weakness in the Windows XP OOBE, including*
- > *retail and OEM versions. Because the Administrator*
- > *account was never requested, this leaves the system*
- > *in a very vulnerable state.*
- >
- > *By using the Computer Management application and*
- > *looking under 'System Tools->Local Users and*
- > *Groups->Users', we see that the Administrator*
- > *account has been added and enabled. This account IS*
- > *NOT password-protected. If the installer sets a*
- > *password for EVERY user shown under the User*
- > *Accounts tool in the Control Panel, THE DEFAULT*
- > *ADMINISTRATOR ACCOUNT STILL EXISTS WITH NO PASSWORD.*
- >
- > *The Installation Setup never informed the user that*
- > *the account existed. If a user attempts to manually*
- > *set a password for the Administrator account, they*
- > *are greeted with the following warning: "Password*
- > *for Administrator: Resetting this password might*
- > *cause irreversible loss of information for this user*
- > *account. For security reasons, Windows protects*
- > *certain information by making it impossible to*
- > *access if the user's password is reset. This data*
- > *loss will occur the next time the user logs off. You*
- > *should use this command only if a user has forgotten*
- > *his or her password and does not have a password*
- > *reset disk. If this user has created a password*
- > *reset disk, then he or she should use that disk to*
- > *set the password. If the user knows the password and*
- > *wants to change it, he or she should log in, then*
- > *press CTRL+ALT+DELETE and click Change Password. For*
- > *additional information, click Help. [Proceed]*
- > *[Cancel] [Help]." This warning exists in all*
- > *versions of Windows XP, but it is not presented from*
- > *the Control Panel Users Accounts tool. If a password*
- > *is changed from the Control Panel's User Accounts*
- > *section, no such warning is issued; but, again, the*
- > *Administrator account is hidden from User Accounts.*
- >
- > *In summary, Due to the lack of an Administrative*
- > *Setup screen for the IBM Windows XP OOBE flow, it is*
- > *more difficult for a security-conscious organization*
- > *to manage a Windows XP-based IBM environment. In*
- > *order to protect a system, several unintuitive*

Full-Disclosure: Re: Vulnerability in IBM Windows XP: default hidden Administrator account allows local Administrator access

> *additional steps must be taken on each systems in*
> *the environment, despite warnings against taking*
> *such steps.*
>
> *SECNAP has tested this situation against IBM Windows*
> *XP RTM, as well as IBM Windows XP SP1. The*
> *vulnerability has existed since IBM began shipping*
> *systems with Windows XP. Due to the recent release*
> *of XP SP2, an opportunity exists for IBM to remedy*
> *this issue in a timely fashion. SECNAP also*
> *recommends that IBM notify all existing registered*
> *clients using the vulnerable systems to upgrade,*
> *possibly to a IBM-released patch, or modified*
> *version of SP2, that would additionally address the*
> *issues.*
>
> *Exploit:*
> -----
> *Local: Press CTRL+ALT+DEL,DEL to get a login prompt.*
> *Enter user name 'Administrator' and NO PASSWORD and*
> *Click OK.*
> *Network: Because remote logins using accounts*
> *without passwords is disabled, it is not typically*
> *possible to login to the system using RDP or remote*
> *shares.*
>
=== message truncated ===

=====

Harrison Gladden <linuxugur80@yahoo.com>
Tel:(515)708-1065

****Shoot for the moon.
Even if you miss, you'll land among the stars.****

Do you Yahoo!?
Read only the mail you want – Yahoo! Mail SpamGuard.
http://promotions.yahoo.com/new_mail

Re: Vulnerability in IBM Windows XP: default hidden Administrator account allows local Administrator access