Windows XP SP3 WINLOGON Registry Content Information Disclosure

by Matthew “j00ru” Jurczyk and Gynvael Coldwind
Hispasec

1. Basic Information

Name	Windows XP SP3 WINLOGON Registry Content Information Disclosure
Class	Design Error
Impact	Low / Medium
Credits	Matthew “j00ru” Jurczyk, Gynvael Coldwind
Discovered	2008-12-20
Published	2010-05-29

2. Abstract

Microsoft Windows XP is a commonly used desktop operating system, released with Service Pack 3 at the time of writing this paper.

The vulnerable system component is *winlogon.exe*. This process is always running with the highest, SYSTEM privileges, thus being a common vulnerability research target. It is responsible for performing actions like loading the user profile, handling and dispatching SAS events, screen saver control and so on. In order to successfully exploit the issue described in this paper, the attacker would be particularly interested in the 1st functionality – setting up the newly logged user’s environment.

When one of the computer users decides to log on the local machine, Winlogon does some basic work – loads the HKEY_CURRENT_USER / CLASSES key into the registry, launches some essential initial processes, sets the environment variables etc.

Using some standard Winlogon behavior, it is possible for a local (as well as remote) attacker to list the registry values from given key and retrieve their contents at the same time. This creates a chance to obtain some sensitive information from registry values that the attacker wouldn’t have access to under normal circumstances – simply everything that the SYSTEM account is able to read (HKLM, private data of any user working on the machine etc).

The affected operating systems are Windows XP SP3 and probably all the prior versions from the WinNT family. As mentioned before, this vulnerability can also be exploited remotely using Windows Telnet Service (the *tlntsrv.exe* process behaves exactly like *winlogon.exe* in the vulnerability context).

3. Vulnerability details

The WINLOGON (*winlogon.exe*) process is one of the most critical Microsoft Windows components, present since its earliest versions. It is responsible for performing various kinds of operations, all related to user-logging process – setting up new user's environment, dispatching special SAS-events (ctrl-alt-del combination), controlling the Window Stations and screensavers available on the system and more. Given the nature of the work it is supposed to do, it is always present with the SYSTEM privileges, apparently having full access to most of the system data, structures, settings etc.

During the exploitation, the attacker shall take advantage of a Windows Registry design bug. The kernel-mode registry engine provides a nice mechanism, called "symbolic linking". As the name suggests, the mechanism makes it possible for any user logged on the machine to create a "symbolic" (invisible for a normal user) connection between the source and destination keys. The functionality itself doesn't reveal any information yet, since it is not possible to enumerate/read values without appropriate rights set, even through any number of symbolic links.

The idea is to use some higher-privileged (SYSTEM or administrator account's) process to use the symbolic link, forwarding to an inaccessible key, and perform some operations on it. The only requirement is that the process should open the desired key in a deterministic way, and (in case of READ operation being performed), pass the obtained data to the low-level user in some way.

Both conditions are accomplished during the environment variables being set up by *winlogon.exe*, since the names together with their values are read from the following key:

HKEY_CURRENT_USER\Environment\

To be more precise, the *userenv.CreateEnvironmentBlock* function is used to initialize the variables basing on registry settings. The above function enumerates the specific key in search of values with the REG_SZ and REG_EXPAND types, respectively adding the environment entries of the following form:

EnumeratedValueName=EnumeratedValueContents

This gives the attacker an easy chance to enumerate and read values from a given key, if he only knows the exact key path. The particular possibilities created by the vulnerability depend on the specifics of the machine being attacked and the data of attacker's interest.

What should be noted is that not only the *winlogon.exe* component can be used as a high-privileged process that sets the environment up – it's the same situation with any other

SYSTEM process running on the local machine and being able to use the *CreateEnvironmentBlock* function on demand.

4. Impact

This vulnerability allows an attacker to read any registry data (except the parts which even SYSTEM account is forbidden to access) from a local or remote machine. The only requirement is to be able to log on the attacked system twice (firstly, to set the registry link and then to make Winlogon enumerate the values).

The impact of a single attack, considering the above conditions, is rated as low/medium.

5. Disclaimer

Copyright by Hispasec