

# Windows 2000 Vulnerability when renaming TsInternetUser (and potentially other accounts)

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-08/0080.html>

---

**From:** Bowden, Zeb (*zbowden\_at\_VT.EDU*)

**Date:** 08/06/03

Date: Wed, 6 Aug 2003 16:37:42 -0400  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Windows 2000 Domain Controller out of the box configuration has a dangerous way of assigning privileges to the TsInternetUser account. If you look in the GptTmpl.inf file of the Default Domain Controller's Policy you will notice that in the SeInteractiveLogonRight item you see a bunch of SIDs and then TsInternetUser (notice NOT domain\TsInternetUser). So TsInternetUser is defined by name in the Default Domain Controller's Policy. Being defined by just the name is necessary for restricted groups but it should not be necessary for an account with a standard RID (1000) like TsInternetUser. Assigning rights by name is dangerous, because that means the name of the object is the only identifier of that object. So if you rename the object, then you'd need to modify the policy to reflect that change.

So what happens if TsInternetUser is renamed?

When rights are assigned by name, the Local Security Authority (LSA) needs to resolve the names to SIDs so it has to look up the SID given only the name of the object (again notice NOT domain\name, just name). LSA will query the GC looking for the SID, passing the name of the object (TsInternetUser) to the LookupAccountName function, which in a multiple domain environment will likely return many SIDs. If there is a TsInternetUser account in your domain LSA will always use it, according to Microsoft PSS. However since we renamed TsInternetUser, it is not returned in our query results from the GC so LSA will just take whichever one is first (which changes). All there is to go by is the name; LSA cannot verify whether Terminal Services Licensing in fact uses the TsInternetUser that it has selected. So if another child domain in your forest named one of their users 'TsInternetUser' for whatever reason, then that user could potentially receive the same rights you intended to be given to the renamed TsInternetUser account in your domain, which by default is 'Logon Locally'.

The problem, we think, occurs when you promote the server to a Domain Controller. When dcpromo.exe is building the Default Domain Controller's Policy, it appears to only assign user rights by name if they are already defined in the server's Local Security Policy. After the server becomes a Domain Controller you can look at the local settings of the Local Security Policy and see rights assigned to 'Domain\user' or 'Domain\group', however in the effective settings (and in the GptTmpl.inf file) you see the rights assigned to just 'user' or 'group'. So just like in the above scenario with TsInternetUser, if you rename or delete 'user' or 'group' and create a new object with the same name it will receive those rights. Also if an object exists already in your forest with the same name it may inherit those rights, depending on the order of the results returned from the GC. Built-in groups do not appear to be vulnerable however; they are defined by their SID in both the effective and local settings of Local Security Policy.

An example of the above paragraph is as follows. On a fresh install of Windows 2000 Server, rename the administrator account to 'myadmin'. Then give 'myadmin' the rights to logon as a batch job and add

