

## RE: Bypass Traverse Checking?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-01/0072.html>

---

**From:** Laura A. Robinson ([larobins@bellatlantic.net](mailto:larobins@bellatlantic.net))

**Date:** 01/24/03

From: "Laura A. Robinson" <[larobins@bellatlantic.net](mailto:larobins@bellatlantic.net)>  
To: "'Hall, Randy'" <[randy.hall@intel.com](mailto:randy.hall@intel.com)>, <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>  
Date: Fri, 24 Jan 2003 17:34:05 -0500

BTW, as a quick side note, I do not wish to imply that Domain Users = Authenticated Users, because they are significantly different (different types of groups, different membership, different capabilities in terms of population), and if an ACL contains only the SID for Authenticated Users, an account without that SID in its token would not be able to access the resource.

So, to reiterate, by changing "Everyone" to "Authenticated Users" in an ACL, you are affecting Anonymous Logon (null connections) and the \_builtin\_ Guest account (one account, not the guest groups). That's it. You are not affecting Guests, nor are you affecting Domain Guests.

Just wanted to make sure I wasn't being unclear. :-)

Laura

> -----Original Message-----  
> **From:** Laura A. Robinson [<mailto:larobins@bellatlantic.net>]  
> **Sent:** Friday, January 24, 2003 5:05 PM  
> **To:** 'Hall, Randy'; '[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)'  
> **Subject:** RE: Bypass Traverse Checking?  
>  
>  
> *Not to drag this out further, and Brett is a friend of mine*  
> *so I don't want to sound like I'm disagreeing, but there's a*  
> *significant distinction that isn't in his article, and there*  
> *is a small incorrect statement, as well.*  
>  
> **Note:** Guest != Guests  
>  
> *If you use the builtin Guest account and log on, this is what*  
> *your access token looks like (the guest account in this*  
> *domain is renamed "Administrator", which you can verify by*  
> *looking at the SID of the account. That was done for*