

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

4/19/97

BUILT-IN ANONYMOUS USER BACK DOOR

ISS Advisory

Problem: A very serious security vulnerability in Windows NT has been discovered and knowledge of it has been made publicly available.

Affects: Any Windows NT host on a network.

Description:

An MWC exploit which demonstrates a security hole in Windows NT has been released. The demonstration reads the registry of a remote machine, and lists the users and shares, even if the currently logged in user has no legitimate access to the target machine. The exploit can be obtained from <http://www.ntsecurity.com>.

The source of the problem is the built-in user known as "anonymous". This user is used by Windows NT for machine to machine communication, and was not previously known to have access to any resources. However, now that it has been demonstrated to be able to access Windows NT resources, it is important to note that "anonymous" is a member of the "everyone" group.

This has a number of implications:

- Any Windows NT machine which has NetBIOS bound to the network can have registry information read or written to the extent that the "everyone" group has access. The full extent of this problem will be explained below.
- The application and system logs (but not the security logs) can also be read.
- Any file share with access to "everyone" (which is the default) can also be accessed.
- Lan Manager calls can be used to enumerate all of the users on the machine, determine which user is the administrator (even if renamed), and list all of the shares.

The extent of the problem with the registry is as follows:

- Most of the keys which are created on install are properly secured, even from everyone. Under a default scenario, everyone does not have permissions to write to most of the registry, and if they do, it is normally only to create sub-keys, not write values. One possibility which was raised was that perhaps shares could be added via the registry - the default permissions will not allow this. It is not good thing to let an intruder read the Windows NT registry, but it is a much more severe problem to allow it to be written.

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

- Just about ANY software installed after OS install will not have correct permissions, and are FULLY writable by everyone. It is suspected that this is because the install scripts expect to be installing into Win95, which has no concept of security. This has been observed with file permissions as well. It would be very possible to utilize this type of access to install trojans, and point applications like browsers, news and mail readers at trojans.

For example:

```
software\Clients\mail\Exchange\shell\open\command  
software\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents
```

and a number of other items which could be subverted are writable.

Solutions:

- If a machine is directly connected to the internet, unbind NetBIOS services from the interface connected to the internet. This would be especially appropriate for Web and FTP servers. This is done by opening Control Panel, Networks, and choosing the Bindings tab.
- ISS has written a small tool which changes "everyone" to "users" for an entire registry tree. The tool is `everyone2users.exe`, and is currently available from <ftp://ftp.iss.net/everyone2users.exe> and <http://ntbugtraq.rc.on.ca/david.htm>.

Usage of the tool is:

everyone2users [registry key to set permissions]

It is recommended that this tool be run as follows:

everyone2users software

and

everyone2users system\currentcontrolset\services

- Evaluate the exposure of any file system shares to "everyone". This can be done by selecting properties of a share from explorer. The Windows NT version of the ISS Internet Scanner also detects shares which are set with full access to everyone, and can be obtained from <http://www.iss.net/eval>.

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

It is unclear at this time how to prevent the users from being listed. It is expected that Microsoft will be patching the problem as rapidly as they can. It is our opinion that this is a serious vulnerability and immediate attention should be paid to preventing an intruder from exploiting this problem. The availability of a demo for this problem substantially reduces the amount of time it will take before the mechanism will become well known. There are also a number of tools which can help identify the extent to which the everyone group has access to a host - see <http://www.somarsoft.com> for several shareware tools which may be helpful.

```
net use \\192.168.202.33\IPC$ "" /user:""
```

KNOWLEGDE BASE Q143474

Restricting Information Available to Anonymous Logon Users

The information in this article applies to:

- Microsoft Windows NT Workstation version 4.0 Service Pack 3
- Microsoft Windows NT Server version 4.0 Service Pack 3
- Microsoft Windows NT Workstation version 3.51
- Microsoft Windows NT Server version 3.51

SUMMARY

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT 3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Listing account names from Domain Controllers is required by the Windows NT ACL editor, for example, to obtain the list of users and groups to select who a user wants to grant access rights. Listing account names is also used by Windows NT Explorer to select from list of users and groups to grant access to a share.

MORE INFORMATION

Windows NT networks based on a single Windows NT domain will always be able to authenticate connections to list domain account information. Windows NT networks that use multiple domains may require anonymous user logon to list account information. A brief example shows how anonymous connections are used. Consider two Windows NT domains, an account domain and a resource domain. The resource domain has a one-way trust relationship with the account domain. That is, the resource domain "trusts" the account domain, but the account domain does not trust the resource domain. Users from the account domain can authenticate and access resources in the resource domain based on the one-way trust. Suppose an administrator in the resource domain wants to grant access to a file to a user from the account domain. They will want to obtain the list of users and

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

groups from the account domain to select a user/group to grant access rights. Since the account domain does not trust the resource domain, the administrator request to obtain the list of users and groups from the resource domain cannot be authenticated. The connection is made using a NULL session to obtain the list of account domain users.

There are similar situations where obtaining account names using an anonymous connection allows the user interface tools, including Windows NT Explorer, User Manager, and ACL editor, to administer and manage access control information across multiple Windows NT domains. Another example is using User Manager in the resource domain to add users from the trusted account domain to a local group. One way to add the account domain user to a local group in the resource domain is to manually enter a known domain\username to add access without getting the complete list of names from the account domain. Another approach is to logon to the system in the resource domain using an account in the trusted account domain.

Windows NT environments that want to restrict anonymous connections from listing account names can control this operation after installing Windows NT 4.0 Service Pack 3 or the Windows NT 3.51 hotfix.

After installation of Windows NT 4.0 Service Pack 3 or the Windows NT 3.51 hotfix, administrators who want to require only authenticated users to list account names, and exclude anonymous connections from doing so, need to make the following change to the registry:

WARNING: Using Registry Editor incorrectly can cause serious, system-wide problems that may require you to reinstall Windows NT to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk.

- 1.Run Registry Editor (Regedt32.exe).

- 2.Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

- 3.On the Edit menu, click Add Value and use the following entry:

Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1

- 4.Exit the Registry Editor and restart the computer for the change to take effect.

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

The purpose of the registry value is to configure local system policy for whether authentication is required to perform common enumeration functions. Requiring authentication to obtain the account name list is an optional feature. When the RestrictAnonymous value is set to 1, anonymous connections from the Graphical User Interface tools for security management will receive an access denied error when attempting to get the list of account names. When the RestrictAnonymous value is set to 0, or the value is not defined, anonymous connections will be able to list account names and enumerate share names. It should be noted that even with the value of RestrictAnonymous set to 1, although the user interface tools with the system will not list account names, there are Win32 programming interfaces to support individual name lookup that do not restrict anonymous connections.

Windows NT networks using a multiple domain model can restrict anonymous connections without loss of functionality. The initial steps in planning to disable anonymous connections is for administrators in resource domains to add members of trusted account domains to specific local groups as needed before changing the value for the LSA RestrictAnonymous registry entry. Users logged on using accounts from trusted account domains will continue to use authenticated connections to obtain list of account names to manage security access control.

Restricting Anonymous List of Share Names

The Server service that provides remote file access to share resources will also use the LSA registry value, RestrictAnonymous, to control whether anonymous connections can obtain a list of share names. Therefore, administrators can set the value of a single registry configuration entry to define how the system responds to enumeration requests by anonymous logons.

Restricting Anonymous Remote Registry Access

Installation of Windows NT 4.0 Service Pack 3 or the Windows NT 3.51 hotfix removes the ability for anonymous users to connect to the registry remotely. Anonymous users cannot connect to the registry and cannot read or write any registry data. As a reminder, Windows NT 4.0 restricts remote access to the registry by domain users using the access control list on the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

The ACL on this key identifies the authenticated users allowed to remotely connect to the registry. Windows NT 4.0 Server, by default, only allows Administrators remote registry access. The winreg\AllowedPaths subkey identifies specific portions of the registry that authenticated users who are not explicitly granted access by the winreg ACL can use for printer access and other system operations. The winreg key may be defined on Windows NT 4.0 Workstations to restrict remote registry access to those systems. For more information on the winreg key, please see the following article in the Microsoft Knowledge Base:

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

ARTICLE-ID: Q155363

TITLE : How To Regulate Network Access to the Windows NT Registry

Authenticated Users Built-in Group

A new built-in group is created when installing Windows NT 4.0 Service Pack 3 or the Windows NT 3.51 hotfix known as "Authenticated Users." The Authenticated Users group is similar to the "Everyone" group, except for one important difference: anonymous logon users (or NULL session connections) are never members of the Authenticated Users group. The built-in Security Identifier for Authenticated Users is S-1-5-11. Authenticated network connections from any account in the server's Windows NT domain, or any domain trusted by the server's domain, is identified as an Authenticated User. The Authenticated Users group is available for granting access rights to resources in the security ACL editor. Windows NT 4.0 Service Pack 3 and the Windows NT 3.51 hotfix do not modify any access control lists to change access rights granted to Everyone to use Authenticated Users.

Windows NT 3.51 Hotfix

The Windows NT 3.51 hotfix has been posted to the following Internet location:

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/hotfixes-postSP5/sec-fix>

Additional query words: 4.00 3.51 sp3 sid

Keywords : kbenv kbnetwork ntsecurity NTSrvWkst

Version : winnt:3.51

Platform : winnt

Issue type : kbinfo

KNOWLEGDE BASE Q155363

HOWTO: Regulate Network Access to the Windows NT Registry

The information in this article applies to:

Microsoft Windows NT 4.0

Microsoft Win32 Software Development Kit (SDK) for Windows NT

Microsoft Windows 2000

SUMMARY

This article describes new functionality in Windows NT 4.0 that provides a system administrator with the ability to secure remote registry access.

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

MORE INFORMATION

Windows NT supports accessing a remote registry via the Registry Editor and also through the RegConnectRegistry() Win32 API call. The default security on the registry allows for easy use and configuration by users in a network. In some cases, it may be useful to regulate who has remote access to the registry, in order to prevent potential security problems.

The security on the following registry key dictates which users/groups can access the registry remotely:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\
winreg

If this key does not exist, remote access is not restricted, and only the underlying security on the individual keys control access.

In a default Windows NT workstation installation, this key does not exist. In a default Windows NT server installation, this key exists and grants administrators full control for remote registry operations.

The following optional subkey defines specific paths into the registry that are allowed access, regardless of the security on the winreg registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\
Winreg\AllowedPaths\Machine (entry of type REG_MULTI_SZ)

The "AllowedPaths" registry key contains multiple strings, which represent registry entries that can be read by Everyone. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the "AllowedPaths" registry key only grants Administrators the ability to manage these paths.

Any changes to the above registry entries require a reboot in order to take effect.

Note that modifying the security and key contents can be performed using the registry editor utility (Regedt32.exe).

The following KB article illustrates how to programmatically access the Windows NT registry and apply security to a registry key:

Q146906 How to Secure Performance Data in Windows NT

Additional query words:

RED BUTTON VULNERABILITY WINDOWS NT

By Mark E. Donaldson

Keywords : kbKernBase kbWinOS2000 kbRegistry kbSecurity kbDSupport

kbGrpKernBase

Version : NT;; WINDOWS;; winnt:4.0

Platform : NT WINDOWS winnt

Issue type : kbhowto