

Re: Security templates and settings in Windows XP

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-12/msg00063.html>

- *From:* "Thor (Hammer of God)" <thor@xxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 28 Dec 2005 16:14:16 -0800
-

If you want to do this via the registry, you'll have to cross-reference the NetCfgInstanceID of the "Packet Scheduler Miniport" in the Network Adapter class to the UpperBindings value referenced PSched service.

Find the reference in

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PSched\Parameters\Adapters for the particular adapter it may be bound to, and check the "Network Adapters" class in

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class (you'll have to find what ID your "Network Adapters" class is...) to see if it is there.

The UID will change each time you bind and unbind the QoS Packet Scheduler from the interface. When you bind it, the appropriate binding is created in Network Adapters and given the NetCfgInstanceID for the interface referenced in the PSched parameters. When you unbind it, that entire class goes away, but the PSched parameters will retain the UID it used to be.

Basically, grab the UID in the PSched parameters and see if it lives in Classes. If not, it's not bound. If so, it is.

If you don't mind, can you tell me SANS' justification for disabling the QoS Packet Scheduler? I only pertains to LAN traffic, and only for cards that support it. Note you can disable QoS percentages via Group Policy using the Network Administrative Templates...

Oh, and if you want to quickly identify the UID of an interface and what transports are bound to it, you can use TransportEnum off my website <http://www.hammerofgod.com/download.htm> --- it will dump the UID of all transports for all active interfaces on a machine. Works on remote machines too, even over an anonymous connection if you follow the exe with \\computername. (It won't work if the client has a fw, of course.)

hth

Re: Security templates and settings in Windows XP

t

"I may disapprove of what you say,
but I will defend to the death your
right to say it."

----- Original Message ----- From: "Bill Busby"
<williambusby2001@xxxxxxxxxx>
To: "Chris Serafin" <chris@xxxxxxxxxxxxxxxxxxxx>;
<focus-ms@xxxxxxxxxxxxxxxxxxxx>
Sent: Wednesday, December 28, 2005 1:03 PM
Subject: RE: Security templates and settings in Windows XP

No I am automating a security check script that checks
to verify that QoS is disabled on Windows XP systems.

--- Chris Serafin <chris@xxxxxxxxxxxxxxxxxxxx> wrote:

Are you worried about users changing the QoS DSCP/IP
PREC fields to expedite
their traffic? If so, you could just strip their
DSCP field to = 0 on the
switch; if it is managed.

Chris Serafin
IT Security / Voice Engineer
chris@xxxxxxxxxxxxxxxxxxxx

-----Original Message-----
From: Bill Busby [<mailto:williambusby2001@xxxxxxxxxx>]

Sent: Wednesday, December 28, 2005 12:22 PM
To: focus-ms@xxxxxxxxxxxxxxxxxxxx

Re: Security templates and settings in Windows XP

Re: Security templates and settings in Windows XP

Subject: Security templates and settings in Windows XP

In setting up Windows XP and securing XP, NIST and SANS recomend disabling QOS from XP. I am trying to find a registry key that for QOS so that this setting can be checked remotely. Does anyone know of such a key?

This is one of the steps towards securing Windows XP.

Thanks,

William

Yahoo! for Good - Make a difference this year.
<http://brand.yahoo.com/cybergivingweek2005/>

Re: Security templates and settings in Windows XP

Yahoo! for Good - Make a difference this year.
<http://brand.yahoo.com/cybergivingweek2005/>

