

RE: How to disable all floppy drives on the network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-12/0016.html>

From: Michael Roach (*mroach_at_hamline.edu*)

Date: 12/10/03

To: "'Leung, Annie LDB:EX'" <annie.leung@bcliqorstores.com>, "'Jannie Hanekom'" <j_hanekom@hotmail.com>
Date: Wed, 10 Dec 2003 15:37:45 -0600

My bet in this case is your husband does not have full administrative rights on the workstation and thus cannot install/add any hardware devices to the system.

-----Original Message-----

From: Leung, Annie LDB:EX [mailto:annie.leung@bcliqorstores.com]
Sent: Wednesday, December 10, 2003 2:41 PM
To: 'Jannie Hanekom'; focus-ms@securityfocus.com
Cc: sakaba@alexandria.cc
Subject: RE: How to disable all floppy drives on the network

FYI.

I bought a USB storage device of 64 MB early this year. I gave it to my husband for him to save his PowerPoint files at work. However, his workstation failed to accept it and he asked their administrator who said it is the company policy that they don't allow these devices and the platform actually configured to not accept these USB devices.

I don't know how do they do that, by workstation or by GPO, don't know.

Annie Leung

-----Original Message-----

From: Jannie Hanekom [mailto:j_hanekom@hotmail.com]
Sent: Wednesday, December 10, 2003 11:02 AM
To: focus-ms@securityfocus.com
Cc: sakaba@alexandria.cc
Subject: RE: How to disable all floppy drives on the network

If you can disable the "Floppy Disk" driver through a policy, you'll probably meet management's requirement, though many would see the logic as flawed. The "Hide these specified drives" user policy is also quite useful in enforcing this type of limit.

Note that disabling the floppy driver doesn't prevent people from sticking in ZIP drives, LS-120 drives, CD Writers, USB Storage Keys, Infrared, USB

SecurityFocus Microsoft: RE: How to disable all floppy drives on the network

Wireless LAN adapters, printers, or any other type of removable storage/transfer mechanism. Hiding drives is somewhat useful for that, but you'll have to disable the Command Prompt in conjunction with that. (Any application that doesn't use the standard Windows File Open/Save/Browse dialogs will still provide access to the removable device.) The floppy disk driver key is at:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Floppydisk

You can change the "Start" type to one of the following:

0x00 Boot
0x01 System
0x02 Auto load
0x03 Load on demand
0x04 Disabled

You can possibly set up your own ADM template for this, but I'm speculating it will be possible to add this into the "System Services" list in Group Policies. Try adding the following into the relevant policy's GptTmpl.inf file in Sysvol\

[Service General Setting]

```
FloppyDisk,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
```

You can get the UUID of the policy by displaying its properties in AD Users & Computers. The line above should add a "FloppyDisk" entry under System Services in the group policy you added it to. Open the Group Policy, change anything (just to notify AD that it has changed) and close it. I've not tested it, but in theory applying the policy now will disable the floppy driver.

Just be careful with applying this policy to all computers – limit "Apply Group Policy" to only a test set of workstations to verify that this actually works.

Jannie

-----Original Message-----

From: Sakaba [mailto:Sakaba@alexandria.cc]

Sent: 10 December 2003 05:46

To: focus-ms@securityfocus.com

Subject: How to disable all floppy drives on the network

Hi everyone,

I got a AD network running mostly Win2k and WinXP. All our client PCs have floppy drives but I've been asked by management to remove them to prevent users from putting data on floppies which short of encrypting the files lack security. This is obviously very time consuming so I'm looking for a way to

RE: How to disable all floppy drives on the network

SecurityFocus Microsoft: RE: How to disable all floppy drives on the network

simply disable them.

– The group policy setting that limits access to the locally logged in user is no good because the drive still shows up to many applications that were installed under local admin.

– I can disable each drive via AD users/computers-->manage computer (one at a time)-->disable floppy device. This is very time consuming because I can't manage multiple computers at a time and we are talking about thousands of boxes.

I was thinking maybe a WMI script might do it but I'm a neopyte in that area so I'm not sure. Any ideas?

Best Regards,
sakaba

