



MOTOROLA
intelligence everywhere™

REMOVING THE NANTSYS.SYS DRIVER FROM NETOCTOPUS WINDOWS AGENTS

netOctopus Windows Agents include a system driver, *nantsys.sys*, that may improperly expose certain kernel functionality. A local application may be able to exploit this driver to elevate its execution privileges or to crash the local system.

The system driver that may allow this exploit is responsible for gathering certain system information, including BIOS vendor information and information about PCI devices. Removing this driver will prevent the netOctopus Agent from gathering this system information, but it will not otherwise affect the Agent's functionality.

Because this system driver is not a critical component of the netOctopus Agent, the best solution to this potential vulnerability is to completely remove the system driver. Motorola is providing a VBScript script that will completely remove the driver and reboot your computer. Execute this script on your netOctopus Agent computers just as you would deploy any other script—use the netOctopus Administrator or deploy it manually.

You may execute this VBScript in two different modes: *attended* and *silent*.

- When the script runs in attended mode, it will display a confirmation dialog box on the Agent computer. It will also return any error messages that may be generated.
- When the script runs in silent mode, no user interface is displayed on the Agent computer. When the script is complete, it will reboot the computer immediately *regardless of what the local user is doing*.

ATTENDED MODE

When the script is executed in attended mode on the Agent computer, the local user will receive a confirmation dialog box. The local user must accept the script before it will run.

If the script generates errors when it runs, the local user will receive an additional dialog box with the message

```
There was a failure in the removal of the nantsys.sys driver.  
Please contact your system administrator for more information.  
Error: <errorstring>
```

<errorstring> can be any of the following phrases.

```
"Failed to initialize!"  
"Failed to stop the service!"  
"Failed to delete the nantsys.sys driver file!"  
"Failed to remove the service!"  
"Failed to reboot the system! The nantsys.sys driver  
file was deleted. To finished this task, you  
must reboot your system manually."
```

Error messages are *not* relayed to the netOctopus Administrator.

SILENT MODE

When the script is executed in silent mode on the Agent computer, no user interface is displayed on the Agent computer. When the script is complete, it will reboot the computer immediately *regardless of what the local user is doing*. Silent mode is intended for use in highly managed environments.

Activate silent mode by passing the */s* parameter to the script from the command line.