



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

January 21, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2009-004

DATE(S) ISSUED:

01/21/09

Microsoft Windows Does Not Disable AutoRun Properly

Source: US-CERT

Systems Affected

* Microsoft Windows

Overview

Disabling AutoRun on Microsoft Windows systems can help prevent the spread of malicious code. However, Microsoft's guidelines for disabling AutoRun are not fully effective, which could be considered a vulnerability.

1. Description

- a. Microsoft Windows includes an AutoRun feature, which can automatically run code when removable devices are connected to the computer. AutoRun (and the closely related AutoPlay) can unexpectedly cause arbitrary code execution in the following situations:
 - i. A removable device is connected to a computer. This includes, but is not limited to, inserting a CD or DVD, connecting a USB or Firewire device, or mapping a network drive. This connection can result in code execution without any additional user interaction.
 - ii. A user clicks the drive icon for a removable device in Windows Explorer. Rather than exploring the drive's contents, this action can cause code execution.
 - iii. The user selects an option from the AutoPlay dialog that is displayed when a removable device is connected. Malicious software, such as W32.Downadup, is using AutoRun to spread. Disabling AutoRun, as specified in the CERT/CC Vulnerability Analysis blog, is an effective way of helping to prevent the spread of malicious code.
 - iv. The Autorun and NoDriveTypeAutorun registry values are both ineffective for fully disabling AutoRun capabilities on Microsoft

Windows systems. Setting the Autorun registry value to 0 will not prevent newly connected devices from automatically running code specified in the Autorun.inf file. It will, however, disable Media Change Notification (MCN) messages, which may prevent Windows from detecting when a CD or DVD is changed. According to Microsoft, setting the NoDriveTypeAutorun registry value to 0xFF "disables Autoplay on all types of drives." Even with this value set, Windows may execute arbitrary code when the user clicks the icon for the device in Windows Explorer.

2. Impact

- a. By placing an Autorun.inf file on a device, an attacker may be able to automatically execute arbitrary code when the device is connected to a Windows system. Code execution may also take place when the user attempts to browse to the software location with Windows Explorer.

3. Solution: Disable AutoRun in Microsoft Windows

- a. To effectively disable AutoRun in Microsoft Windows, import the following registry value:

- i. REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf]
@=" @SYS:DoesNotExist"

- ii. To import this value, perform the following steps:

1. Copy the text
2. Paste the text into Windows Notepad
3. Save the file as autorun.reg
4. Navigate to the file location
5. Double-click the file to import it into the Windows registry

- b. Microsoft Windows can also cache the AutoRun information from mounted devices in the MountPoints2 registry key. We recommend restarting Windows after making the registry change so that any cached mount points are reinitialized in a way that ignores the Autorun.inf file. Alternatively, the following registry key may be deleted:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- c. Once these changes have been made, all of the AutoRun code execution scenarios described above will be mitigated because Windows will no longer parse Autorun.inf files to determine which actions to take. Further details are available in the CERT/CC Vulnerability Analysis blog. Thanks to Nick Brown and Emin Atac for providing the workaround.

4. References

- a. The Dangers of Windows AutoRun - http://www.cert.org/blogs/vuls/2008/04/the_dangers_of_windows_autorun.html

- b. US-CERT Vulnerability Note VU#889747 -
<<http://www.kb.cert.org/vuls/id/889747>>
- c. Nick Brown's blog: Memory stick worms -
<<http://nick.brown.free.fr/blog/2007/10/memory-stick-worms>>
- d. TR08-004 Disabling Autorun -
<<http://www.publicsafety.gc.ca/prq/em/ccirc/2008/tr08-004-eng.aspx>>
- e. How to Enable or Disable Automatically Running CD-ROMs -
<<http://support.microsoft.com/kb/155217>>
- f. NoDriveTypeAutoRun -
<<http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/recovery/91525.mspx>>