

Full-Disclosure: Re: [Full-Disclosure] found suspicious desktop.ini in startup folders

Re: [Full-Disclosure] found suspicious desktop.ini in startup folders

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/1119.html>

From: Andrew (aburns_at_premtech.com)

Date: 08/24/04

Date: Tue, 24 Aug 2004 09:55:59 -0500

I actually switched to a OS X PDC and had the same problem when establishing a user's initial login with a windows XP workstation rather than a windows 2k workstation.

It was just a file XP put into the users' profile, and as the knowledge base said, just delete it from the profile on your server should fix the problem. If I recall correctly the reason it shows up is the differences in how the desktop is handled in roaming profiles between WinXP and Win2k. The company I work for is very small, and so I'm not positive on the differences for win2k3

Andrew

On Aug 24, 2004, at 3:35 AM, Nick FitzGerald wrote:

> *BillyBobKnob* wrote:

>

>> *Does anyone know if this file is used in an exploit since it was found in*

>> *startup folders ?*

>

> *Does it "come back" following a restart, or a logout/login cycle, after you delete it??*

>

>> *The contents of the file are:*

>>

>> *[.ShellClassInfo]*

>> *LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21787*

>

> *This KnowledgeBase article mentions precisely these file contents:*

>

> <http://support.microsoft.com/?id=330132>

>

> *but gives no indication of what may cause its appearance on your system. The suggested "fix" is simply deletion...*

>

>

Re: [Full-Disclosure] found suspicious desktop.ini in startup folders

Full-Disclosure: Re: [Full-Disclosure] found suspicious desktop.ini in startup folders

> *Regards,*

>

> *Nick FitzGerald*

>

>

> _____
> *Full-Disclosure – We believe in it.*

> *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*

>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>