

RE: IIS still vulnerable

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-12/0696.html>

From: Christopher Haun (*a-chaun_at_NOSPAMmicrosoft.com*)

Date: 12/29/03

Date: Mon, 29 Dec 2003 18:55:07 GMT

Yes, definitely lock permissions down on the ntfs level for the iusr account if using anonymous access on any ftp sites. These kb articles should help show the minimum levels.

187506 INFO: Basic NTFS Permissions for IIS 4.0

<http://support.microsoft.com/?id=187506>

271071 HOW TO: Set Basic NTFS Permissions for IIS 5.0

<http://support.microsoft.com/?id=271071>

812614 INFO: Default Permissions and User Rights for IIS 6.0

<http://support.microsoft.com/?id=812614>

Also consider looking at the ftp properties to lock down the site(s) with certain ip address exclusions. The IIS logs (start > run > logfiles) may show his IP address. Then you can lock him out that way.

Keep in mind that the intruder may have installed some more backdoors on the system.

On the surface it doesn't sound like the intruder is very malevolent.

However, it may not be worth giving him the benefit of the doubt.

There is some good general advice at:

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

Hope that helps,

Chris – IIS Team