

Re: Secured IIS Project – IIS 4.0 Secure Script

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-07/0010.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 07/24/01

Message-ID: <E9A01F52DC939448BBDE44ED2E1C468F167ACB@muskie.rc.on.ca>
Date: Tue, 24 Jul 2001 12:08:12 -0400
From: Russ <Russ.Cooper@RC.ON.CA>
Subject: Re: Secured IIS Project - IIS 4.0 Secure Script
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

-----BEGIN PGP SIGNED MESSAGE-----

I've completed v1.0 of SecuredIIS.vbs, a Visual Basic script;
<http://ntbugtraq.ntadvice.com/download/SecuredIIS.zip>

which, using Windows Scripting Host, implements many of the
recommendations from the;

Microsoft Internet Information Server 4.0 Security Checklist
<http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp>

plus additional things I felt were prudent.

The intent of this script is that it be given to owners of, and run
on, IIS 4.0 servers which have been installed accepting the defaults.
It should operate identically on NT 4.0 machines which have installed
IIS 4.0 from the NT 4.0 Option Kit using the "Typical" installation
of NTOK.

Machines which were upgraded from IIS 2.0 (original NT installation),
or IIS 3.0 may have remnants left behind which we'd like to remove
(anyone noticing anything on such machines, please drop me a note).

The basic system used for testing here is;

NT 4.0 (no IIS)
NT 4.0 SP6a 128-bit
IE 4.0 SP2 (typical)
NT 4.0 Option Kit (typical)
MDAC_TYP (MDAC 2.1 upgrade)
NT 4.0 SP6a 128-bit

This setup creates an SMTP server, FTP server, Index Server, Windows

NT-Bugtraq: Re: Secured IIS Project – IIS 4.0 Secure Script

Scripting Host (required for the script to work, but part of a default installation of NTOK), and FrontPage extensions.

The script isn't intended to ask questions or provide options. If someone has sufficient knowledge to know what they want, or don't want, from their installation then they should be reading the Security Checklist above or altering their installation via the NTOK Setup program. Those that don't know, or don't want to know, can just double-click on the