Center for Internet Security Benchmark for IIS 5.0 and 6.0 for Microsoft Windows 2000, XP, and Server 2003

Version 1.0

August 15, 2007

Editor: Shyama Rose
Leviathan Security Group

http://cisecurity.org
cis-feedback@cisecurity.org

Table of Contents

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer

or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this

paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 – 02/20/04

Introduction

This benchmark is based on research conducted utilizing Internet Information Services 5.0 on Windows 2000 and XP, and IIS 6 on Windows 2003 Server. It defines a set of rules and settings for a secure installation, setup, and configuration. The set of rules constitute a benchmark. This benchmark represents an industry consensus of "best practices" listing steps to be taken as well as rationale for their recommendation.

This IIS benchmark contains information on securing components including: services installed or enabled by IIS, legacy settings containing insecure by default settings, such as Default files, registry and files and directories, and Metabase settings containing configuration values such as anonymous user name, authflags and others. Finally it contains ASP .NET settings that pertain to how a web application behaves such as authentication, custom errors, etc.

Applicability

This document is intended for those attempting to secure IIS 5.0 on Windows 2000 and XP, and IIS 6 on Windows 2003 Server.

1 - Legacy IIS settings

IIS version 5.0 and 5.1 contain insecure features by default. Starting with Windows 2003, Microsoft took steps to ensure a "secure by default" configuration.

1.1 Default Install Files

Several sample and/or default files are installed by default with IIS 5 and 5.1.

Discussion:

Removing unnecessary files and folders will help to reduce attack surface thus mitigating unnecessary attack vectors.

Remediation:

It is recommended the "Default Web Site" site not be used and a new site be created. All default Virtual Directories and subsequently some of the files and/or folders they point to should be removed. Below is a short list of the Virtual Directories and default files installed by default that are recommended for removal:

1. Remove the contents of the *inetpub\wwwroot* folder
2. Remove the *inetpub/scripts* folder
3. Remove the */scripts* Virtual Directory mapping if it exists
4. Remove the *inetpub/scripts/IISSamples* folder
5. Remove the */iissamples* Virtual Directory mapping if it exists
6. Restrict access to the *iisadmpwd* Virtual Directory to Windows Authenticated users if it exist or remove the virtual directory mapping
7. Remove the */IISHelp* Virtual Directory mapping if it exists
8. Remove the */Printers* Virtual Directory mapping if it exists

1.2 Remote Data Services (RDS)

The Remote Data Services (RDS) component enables controlled Internet access through IIS to remote data resources by allowing the retrieval of data from a database server. Its interface is provided by Msadcs.dll, which is located in the following directory: Program Files\Common Files\System\Msadc

Discussion:

A vulnerability in this feature led to the development of the virii and worms such as Code Red and Nimda. Enabling data services over an internet protocol increases security ramifications, and this feature must be secured if it is in use, or removed if it is not being used.

Remediation:

The following steps should be taken to secure RDS:

1. Delete the MSADC samples located in \Progam Files\Common Files\System\Msadc\Samples
2. Remove the registry key located in HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
3. Create a HandlerRequired registry key here: HKLM\Software\Microsoft\DataFactory\HandlerInfo\
4. Create a DWORD = 1 value (safe mode).

The following steps should be taken to remove the MSADC feature:

1. Remove the /MSADC virtual directory mapping from IIS.
2. Remove the RDS files and subdirectories at the following location: \Program Files\Common Files\System\Msadc

1.3 Internet Printing

Printers that are shared on Windows based servers are made accessible to any client computer through this protocol.

Discussion:

Enabled Internet Printing Protocol on the Windows 2000 server (and above) creates an attack vector in which printers attached to the server are accessible through a web page. Patches are available for remotely exploitable buffer overflows in version of IIS 5.0. Internet Printing is also know as web based printing.

Remediation:

Internet Print can be disabled via a local/group policy object or directly through the registry. To disable Internet Printing in the Registry, change the Value data to 0x1. The default setting is null.

HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting
Value name: DisableWebPrinting
Value type: REG_DWORD
Value data: 0x1

Additionally the Internet Printing Protocol script mappings should be removed (see below).

See also:
http://msdn.microsoft.com/library/en-us/gp/gpref.asp

1.4 URLScan

URLScan distills all incoming requests to the server through filtering the requests based on rules that are set by the administrator. This action helps secure the server by arranging that only authentic requests are processed.

Discussion:

URLScan is particularly useful for IIS 5.0 web servers. IIS 6.0 however implements a number of these features by default and therefore may not necessarily gain any additional security (see http://www.microsoft.com/technet/security/tools/urlscan.mspx#EXE).

It is recommended that URLScan be installed for IIS 5.0. Installing and running the URLScan tool will help prevent malicious requests from reaching a server.

Remediation:

Install and run the URLScan tool.

1.5 IIS Lockdown

The IIS Lockdown tool can be used to provide in-depth defense by providing URLScan integration, and removing or disabling IIS services. The tool removes the following directories from the server: IIS Samples, MSADC, IISHelp, Scripts, IISAdmin. Lockdown disables WebDAV and adds the default anonymous Internet user account (IUSR_MACHINE) to Web Anonymous Users and the IWAM_MACHINE account to Web Applications. IIS Lockdown is available from Microsoft at http://www.microsoft.com/technet/security/tools/locktool.mspx. The URLScan tool is now available with the IIS Lockdown tool.

NOTE: The IIS Lockdown automates many of the hardening steps listed in this document. The default settings for IIS 6.0 should not require hardening. Care should be taken when using this tool as it can dramatically reduce usability.

Discussion:

The IIS Lockdown tool reduces the attack surface of IIS-dependent Microsoft products by disabling unnecessary features such as FTP, SMTP, and NNTP.

Remediation:

Install and run the IIS Lockdown tool. Follow the Lockdown configuration tool.

2 - IIS Configuration (Services)

This section contains information on how to secure service components installed by IIS. These services include FTP, SMTP, Frontpage extensions, WebDAV, and SSL. These services can be considered risky from a security perspective and therefore it is recommended to apply security hardening. IIS services that have not been hardened can lead to unauthorized third party relaying, compromise of mail services. The following recommendations are provided for hardening services within IIS.

The following settings can be achieved using the IIS Manager in IIS 6.0 which can be launched using several means. It can be reached by pointing to Administrative Tools from the start menu, then clicking Internet Information Services (IIS) Manager. To start the IIS Manager from the run dialog box, click Start, and then run. Type in **inetmgr** and click **ok**. The IIS Manager can also be launched from the Computer Management Window right clicking on **My Computer** from the start menu and clicking **manage**. Expand the **Services and Applications** node, and click on **Internet Information Services**.

2.1 FTP User Isolation

The FTP (File Transfer Protocol) service provides the ability for users to copy files to and from the server on a network that uses TCP/IP. In order to secure sites, a method called User Isolation is provided. Implement this recommendation if there exists multiple FTP sites and user isolation is preferred and/or required. This property can be enabled or disabled per site with the following levels of authentication:

1. **No isolation:** Does not enable user isolation.
2. **Isolation:** Enables isolation by authenticating against local or domain accounts.
3. **Active Directory Isolation:** Enables isolation by authenticating against an Active Directory container**.**

Discussion:

FTP User Isolation provides the ability to separate users between sites by disallowing users from viewing or modifying other user's content. This feature corrals users into their own directories disallowing them to navigate beyond their own directories. A user's directory will appear as the root of the site, thus restricting access farther up the directory tree.

Remediation:

To add isolated users to an FTP site using domain or local users:

1. For domain users, create a subdirectory under the FTP home directory for each domain accessing the site. Create a subdirectory under the corresponding domain-named subdirectory for each user.
2. For local accounts, create a subdirectory named **Public** under **LocalUser**. For anonymous users, move content to the **Public** subdirectory. Create a subdirectory under **LocalUser** with the user account name.

To add isolated users to an FTP site using Active Directory Mode set the following properties in the metabase:

1. Set UserIsolationMode to 2.
2. Set ADConnectionUserName to the user (Domain\UserName) who has permissions to read Active Directory properties
3. Set the DefaultLogonDomain
4. Set AccessFlags properties, for example: AccessFlags=AccessRead|AccessNoPhysicalDir

2.2 SMTP

SMTP (Simple Mail Transfer Protocol) is a standard service provided over TCP/IP used for sending and receiving messages from one computer to another on a network. IIS supports this component by sending or receiving email messages.

Discussion:

Securing SMTP involves requiring users to authenticate to the SMTP server before relaying messages, setting operator permissions, and requiring TLS (Transport Layer Security) encryption.

Remediation:

SMTP authenticates using several methods: clear text, and windows authentication. It is recommended to use Windows authentication. To require authentication for incoming and outgoing connections, take the following steps:

1. In the IIS Manager, right click on the SMTP virtual server and choose **Properties**
2. Select the **Access** tab and under **Access Control** click **Authentication**.
3. Select the **Integrated Windows Authentication** checkbox

To add relay restrictions to an SMTP virtual server, perform the following steps:

1. In the IIS Manager on the **Access** tab, click **Relay**
2. In the **Relay Restrictions** box choose **Add**.
3. To add a single computer, click Single computer, type the IP address of the computer to add, and then click OK.

4. To add a group of computers, click Group of computers, type the subnet address and the subnet mask of the group into the corresponding boxes, and then click OK
5. To add a domain, click Domain, type the domain name to add, and then click OK.

The following steps will grant user accounts with operator permissions for the SMTP virtual server:

1. In the IIS Manager, right click on the SMTP virtual server and choose **Properties**
2. Select the **Security** tab, and click Add
3. Select a Windows user account, and then click OK.

To require TLS encryption, it is required to first create a key/pair and configure key certificates, and then set the encryption levels for the server.

1. In the IIS Manager, right click on the SMTP virtual server and choose **Properties**
2. Select the **Access** tab, and under **Secure communication**, click **Certificate** to set up new key certificates and manage installed key certificates for the SMTP virtual server.
3. Select the **Access** tab, and under **Access control**, click **Authentication**.
4. Select the **Require TLS encryption** box.

2.3 SSL

SSL (Secure Socket Layer) can provide encrypted network transmissions using a public and private key system to encrypt data that is transferred over a connection.

Discussion:

Use SSL when passing secure information such as credit card information over a channel.

Remediation:

To enable SSL on a server, take the following steps:

1. In IIS Manager, double-click the local computer, and then double-click the Web Sites folder
2. Right-click the Web site or file to protect with SSL, and then click Properties
3. Select **Advanced**
4. In the Advanced Web site identification box, under Multiple identities for this Web site, verify that the Web site IP address is assigned to port 443, the default port for secure communications, and then click OK. Optionally, to configure more SSL ports for this Web site, click Add under Multiple identities of this Web site, and then click OK
5. Click Edit on the Directory Security or File Security tab, under Secure communications,

6. In the Secure Communications box, select the Require secure channel (SSL) check box
7. To enable SSL client certificate authentication and mapping features, select the Enable client certificate mapping check box, click Edit, add the 1-to-1 or many-to-1 mappings needed, and then click OK three times

2.4 Worker Process Identities

A worker process identity runs under a built-in Network Service account. IIS 6.0 provides the option to use one of the three pre-defined accounts, or create an entirely new account.

Discussion:

Applications that use worker process identities have a reduced attack surface when an application has been compromised because they have a limited set of privileges and permissions.

Remediation:

To configure a worker process identity using a predefined account, take the following steps:

1. In IIS Manager, expand the local computer, expand the Application Pools folder
2. Right-click the application pool to configure
3. Click Properties.
4. Click the Identity tab.
5. Click Predefined, and in the list box beside it, click Network Service, Local Service, or Local System. Click OK

To configure a worker process identity using a configurable account, take the following steps:

1. In IIS Manager, expand the local computer, expand the Application Pools folder
2. Right-click the application pool to configure
3. Click Configurable.
4. Click Browse, and under Enter the object name to select, type the account name in which the worker process will run under, and then click OK.
5. In the Password box, type the password associated with this account. If there is no password associated with the account, leave the Password box blank
6. Click OK.
7. Add the account just created to the IIS_WPG group

2.5 WebDAV Authentication

WebDAV is a file sharing protocol similar to FTP that is commonly used in Windows Internet-related applications. It allows for the downloading, uploading, and management of files on remote computers across Intranets and the Internet. The type of authentication used per WebDAV share is dependent upon the needs of the server.

Discussion:

WebDAV utilizes authentication and encryption, a feature that FTP does not utilize. Client connections to WebDAV shares should be authenticated. The type of authentication modes available are: Kerberos, Anonymous, Basic Authentication, Digest Authentication, Advanced Digest Authentication, Integrated Windows Authentication, and .NET Passport Authentication.

Remediation:

It is recommended to use at least Windows authentication on WebDAV shares

To configure Integrated Windows Authentication on a WebDAV share, take the following steps:

1. In IIS Manager, double-click the local computer; right-click the Web Sites folder, an individual Web site folder, a virtual directory, or a file; and then click Properties.
2. Click the Directory Security or File Security tab, and then, in the Authentication and access control section, click Edit.
3. In the Authenticated access section, select the Windows Integrated Authentication check box
4. Click OK twice

3 - IIS Configuration (MetaBase)

The MetaBase is designed as a repository for Internet Information Services configuration values. In IIS 6.0, the MetaBase is contained within the following files: MetaBase.xml and MBSchema.xml in the systemroot\System32\Inetsrv folder. The MetaBase.xml file stores IIS configuration information.

MetaBase files of earlier versions (5.0 and earlier) are located within MetaBase.bin in the systemroot\System32\Inetsrv folder.

These files can be edited programmatically or the effective setting can be manipulated through the IIS MMC Snap-in / IIS Admin Tool. To access the IIS MMC Snap-in:

1. Click Start→Run.
2. In the open box, type "mmc" and press OK.
3. Once the MMC console opens, select File→Add / Remove Snap-ins.
4. Click the Add button.
5. Select "Internet Information Services" from the list and press the Add button.
6. Click OK.

Additionally Microsoft provides tools such as MetaEdit and adsutil.vbs which can be used to view/edit settings directly.

References: http://msdn2.microsoft.com/en-us/library/ms525644.aspx, http://support.microsoft.com/kb/232068, http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/d3df4bc9-0954-459a-b5e6-7a8bc462960c.mspx?mfr=true

3.1 Anonymous User (anonymousUserName)

The anonymousUserName property specifies the user context for anonymous users browsing the affected site. All non-application pool IIS threads instantiated by anonymous users will run as the user specified by the anonymousUserName.

Discussion:

The principle of a non-privileged user is one that is running under least privilege, meaning they are non-admin users with limited functionality. The purpose of this is grant an anonymous user the least amount of privileges possibly limiting the actions that this user may perform and therefore reducing the amount of damage in the event of a compromise. This practice lowers the attack surface of a system.

Remediation:

The user specified by this property should be a non-privileged account. By default the IUSR_*machinename* account is created for this purpose.

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. In the Master Properties drop-down list, click the service in question, and then choose Edit.
5. Choose Configuration in the Application Settings box.
6. Select the App Options tab.
7. Disable Anonymous Connections
8. Enter a custom valid user name for anonymous connections
9. Click OK twice to return to the Microsoft Management Console.

3.2 Client-side Application Debugging (AppAllowClientDebug)

The AppAllowClientDebug property indicates whether client-side debugging is allowed.

Discussion:

When this option is enabled detailed debugging information is sent to the end-user's browser. This could lead to information disclosure which could be utilized by a malicious attacker.

Remediation:

It is recommended that the setting for this property be set to "FALSE".

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration in the Application Settings box.
6. Click the Debugging Tab
7. Clear the "Enable ASP client-side script debugging" Setting
8. Click OK twice to return to the Microsoft Management Console.

3.3 Server-Side Application Debugging (AppAllowDebugging)

The AppAllowDebugging property allows server-side debugging.

Discussion:

Disallowing server-side application debugging will prevent users from debugging the application.

Remediation:

The recommended setting for this property is "FALSE".

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration in the Application Settings box.
6. Click the Debugging Tab
7. Clear the "Enable ASP server-side script debugging" Setting
8. Click OK twice to return to the Microsoft Management Console.

3.4 ASP Parent Paths (AspEnableParentPaths)

The AspEnableParentPaths property allows or disallows an ASP page to traverse relative to its directory. In IIS 6.0, this property is disabled by default.

This settings allows the "../" notation to be used in paths. Enabling this features could allow for directory traversal attacks

Discussion:

Setting this property to false will disallow an ASP page to traverse relative to its directory when calling scripts.

Remediation:

The recommended setting for this property is "FALSE". Scripts should be referred to by the absolute or relative path.

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration in the Application Settings box.
6. Click the App Options tab.
7. Clear the Enable Parent Paths option.
8. Click OK twice to return to the Microsoft Management Console.

3.5 Logging to Windows Event Log (AspLogErrorRequests)

The AspLogErrorRequests property specifies whether the web server writes ASP errors to a Windows event log. IIS logs provide several formats for log options: W3C, ODBC, NCSA, and Microsoft IIS log file format. These formats allow for easier dissemination of large portions of logged information on the activity of the IIS server. IIS logs have the capability to log extensive information such as user activity, and Windows systems include a tool called PerfMon which provides supplemental information for IIS logging. It is also recommended to set the path to log files to a non-system drive which can prevent the loss of availability due to the loss of a system drive

Discussion:

IIS logging provides more extensive logging capabilities than the Windows Event log and the various logging formats allow for easier manipulation of the log files.

Remediation:

It is recommended that this setting be set to "False" to allow for IIS logging. Set the path of log files to a non-system drive.

This setting can only be accessed programmatically and can not be accessed through the IIS MMC Snap-in.

3.6 ASP Error Messages Setting (AspScriptErrorSentToBrowser)

The AspScriptErrorSentToBrowser property specifies whether debugging information is returned to the user. When AspScriptErrorSentToBrowser is enabled, users may see extraneous and unnecessary debugging information.

Discussion:

Setting this property to "FALSE" will prevent detailed error information from being sent to the client.

Remediation:

The recommended setting for this property is "FALSE"

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration button in the Application Settings box.

6. Click the Debugging Tab
7. Select the "Send text error message to client" option
8. Click OK twice to return to the Microsoft Management Console.

3.7 Custom ASP Error Message (AspScriptErrorMessage)

When set to false, AspScriptErrorSentToBrowser specifies the error message to send to the browser.

Discussion:

Changing this value from the default prevents a number of automated scanners from detecting that an error has occurred.

Remediation:

This property should be a custom string that displays as little information to the user as possible.

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration button in the Application Settings box.
6. Click the Debugging Tab
7. Enter a custom message in the box below "Send text error message to client"
8. Click OK twice to return to the Microsoft Management Console.

3.8 ASP Session Object Timeout (AspSessionTimeout)

The AspSessionTimeout property configures the default amount of time in which Session objects are maintained after the last request associated with the object is made.

Discussion:

Setting the AspSessionTimeout property will prevent session objects from using extraneously consuming memory resources as well as minimizing session replay attacks.

Remediation:

This setting should remain at a low value to limit the potential for session replay attacks. The IIS 6.0 default value of 10 minutes should provide an acceptable balance of usability and security. IIS 5.1 defaults to 20 minutes and therefore should be changed.

To change this value in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration in the Application Settings box.
6. Click Options Tab
7. Enter a "Session timeout" value
8. Click OK twice to return to the Microsoft Management Console.

3.9 Authentication Flags (AuthFlags)

The AuthFlags property specifies the authentication level required for a given web root or virtual directory.

Discussion:

Setting the appropriate authentication level can protect against inappropriate levels of access for web roots or virtual directories.

Remediation:

Add the appropriate attributes for virtual directories and web roots. The authentication flag attributes are: AuthAnonymous, AuthBasic, AuthMD5, AuthNTLM, AuthPassport. The AuthFlags attributes are defined as follows:

- AuthAnonymous: Allow no authentication to be used to access the resource.
- AuthBasic: Allow HTTP Basic authentication to be used to access the resource. With HTTP Basic authentication Username and password are sent in clear text. Transport Layer Encryption should be used if this is enabled to protect these credentials.
- AuthMD5: Allow HTTP digest form authentication to be used to access the resource. Digest form credentials are liable to brute-force attacks. Transport Layer Encryption should be used if this is enabled to protect these credentials.
- AuthNTLM: Allow Integrated Windows (NTLM) Authentication to be used to access the resource. NTLM credentials are more difficult to brute-force than MD5, but it still susceptible to brute-force attacks. Transport Layer Encryption should be used if this is enabled.
- AuthPassport: Allow passport authentication mechanism to be used for access to the resource.

To change this setting in the IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.

3. Select Properties on the pop-up menu.
4. Click the Directory Security tab.
5. Under "Anonymous Access and Authentication controls" click the Edit button
6. Select Options as appropriate
7. Click OK twice to return to the Microsoft Management Console.

3.10 HTTP Connection Timeout (ConnectionTimeout and ServerListenTimeout)

The ConnectionTimeout (IIS 6.0) and ServerListenTimeout (IIS 5.x) properties specifies the amount of time in seconds that the server will wait before closing an dormant connection.

Discussion:

The ConnectionTimeout and ServerListenTimeout properties will protect against session stealing attacks.

Remediation:

Reduce the value of ConnectionTimeout can help mitigate Denial of Service attacks. In IIS 6.0 the default value is 120. The recommended setting is 120 seconds for individual Web and FTP sites; and 10 minutes for other sites.

To change this setting in the IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site in question.
3. Select Properties on the pop-up menu.
4. Click the Web Site tab.
5. Modify the value in the "Connection Timeout" box
6. Click OK to return to the Microsoft Management Console.

3.11 Directory Browsing (DirBrowseFlags)

The DirBrowseFlags property contains flags to determine whether Directory browsing is enabled. It also determines whether there is a default page in the directory. This setting can be set in virtual directories, so all occurrences need to be checked.

Discussion:

If Directory Browsing is disabled a listing of all files / sub-directories in the current directory will not be returned to the end user

Remediation:

It is recommended that this property be set to "0x40000000", which equates to Directory browsing disable, all directory browsing options disabled and default document enabled.

To change this setting in the IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Clear the "Directory Browsing" option
6. Click the Document Tab
7. Set the "Enable Default Document" option
8. Click OK to return to the Microsoft Management Console.
9. (Repeat as necessary for Virtual and sub-Directories)

3.12 FrontPage Extensions Disable (FrontPageWeb)

The FrontPageWeb property enables or disables FrontPage extensions. Note this option is only present if the FrontPage extensions have been installed.

Discussion:

It is recommended to disable FrontPage extensions because they greatly increase the attack surface of the web server and historically have presented numerous vulnerabilities.

Remediation:

Set this property to "false" to delete all FrontPage extension pages for the affected web site and uninstall FrontPage extensions. Due to the fact that as of late 2006 FrontPage has been discontinued, it is recommended that FrontPage Extensions not be utilized in a production environment.

3.13 Custom HTTP Error Messages (HTTPErrors)

The HTTPErrors property specifies a string, Html file or Url to send to clients for various HTTP errors.

Discussion:

Custom HTTP error messages should be used to display error messages. Using the default error pages increases the reliability of certain automated web scanners due to the presence of known text when a given error occurs.

Remediation:

To change this setting in the IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the "Custom Errors" tab.
5. For each HTTP Error create an Html page which an appropriate message
6. (Repeat as necessary for Virtual and sub-Directories)

3.14 In Process ISAPI DLL (InProcessIsapiApps)

A list of ISAPI filters and extensions is specified by this MetaBase property.

Discussion:

Removing unnecessary DLLs can reduce attack surface.

Remediation:

Remove all unused DLLs from this list. For example, remove the following DLLs if they are not used:

- idq.dll: Indexing Service
- httpext.dll: WebDAV
- httpodbc.dll: Internet Database Connector
- ssinc.dll: Server-Side Include Directives
- msw3prt.dll: HTTP print server
- author.dll: Implements operations such as uploading files, renaming and deleting documents, etc.
- admin.dll: Implements operations such as managing users through FrontPage, etc.
- shtml.dll: Parses server extensions such as browse-time functionality, etc.

This value can only be changed in the MetaBase

3.15 Logging Options (LogExtFileFlags)

This property contains flags which can be used to specify which information is written to a log file or an ODBC store.

Discussion:

Setting the LogExtFileFlags property in the MetaBase on sites can log detailed event information such as visitor information, content visited, etc

LogExtFileBytesRecv, LogExtFileBytesSent, LogExtFileClientIp, LogExtFileComputerName, LogExtFileCookie, LogExtFileDate, LogExtFileFlags, LogExtFileHttpStatus, LogExtFileMethod, LogExtFileReferer, LogExtFileServerIp, LogExtFileServerPort, LogExtFileSiteName, LogExtFileTime, LogExtFileTimeTaken, LogExtFileUriQuery, LogExtFileUriStem, LogExtFileUserAgent, LogExtFileUserName, LogExtFileWin32Status

Remediation:

To change this setting in the IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Select the "Web Site' tab.
5. Under the Logging section click the properties button
6. Click the Extended Properties Tab
7. Select options as appropriate

3.16 Local Path (Path)

The path property specifies a particular hive of the MetaBase. It is a directive for configuring the webroot or a virtual directory path. Having the path on the same drive as the system folder compounds potential attacks such as drive space exhaustion or directory traversal.

Discussion:

Locating the path on a non-system drive helps mitigate directory traversal and other types A secure path would not be located on a system drive.

Remediation:

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Modify the box labeled "Local Path" as needed
6. Click OK to return to the Microsoft Management Console.

3.17 Script Mappings (ScriptMaps)

The ScriptMaps property specifies the file name extensions used for script processor mapping.

Discussion:

Disabling script processor maps which are not being used reduces the attack surface.

Remediation:

Only the required script processor maps should be enabled. Disable script processor maps that are not being used. The "1" flag denotes an allowed extension and the "0" flag denotes a disallowed extension.

The string is represented in the following format:
[Extension], [ScriptProcessor], [Flags], [IncludedVerbs]

In IIS 5.x, if no verbs are listed, it is assumed that "all verbs" is the value, therefore it is important to explicitly list all verbs that the ISAPI extension is to handle. Also, it is recommended to restrict which verbs can be used within an extension.

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Right-click on the Web site / Virtual Directory in question.
3. Select Properties on the pop-up menu.
4. Click the Home Directory / Virtual Directory tab.
5. Select Configuration button in the Application Settings box.
6. Click the Mappings Tab
7. Remove all unnecessary script mappings
8. Click OK twice to return to the Microsoft Management Console.

3.18 Use Hostname in Redirects (UseHostName)

This property specifies to the server to returns the DNS host name.

Discussion:

The UseHostName property will prevent IIS from revealing internal IP addresses when performing redirects.

Remediation:

The recommended setting for this property is TRUE.

This setting can not be changed through the IIS Admin Tool.

To change this property, set UseHostName="TRUE" in the MetaBase.

3.19 Application Pool Identity (WAMUserName)

This property specifies an account used as the COM+ application identity for newly created out-of-process applications.

Discussion:

Setting the WAMUserName to an account with least privileges will limit the actions that this user may perform and therefore reducing the amount of damage in the event of a compromise.

Remediation:

The user specified by this property should be a non-privileged account. By default this value is IWAM_*machinename* (where machine name is the hostname), which is by default a non-privileged account.

In IIS 5.1 and earlier this option is only configurable via the MetaBase.

These settings can be changed in IIS 6.0 with the following configuration.

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Click "Application Pools"
3. Right click on the Application Pool in question
4. Select Properties on the pop-up menu.
5. Click on the Identity Tab
6. Select the configurable option and enter a non-privileged account name in the User Name field
7. Click OK to return to the Microsoft Management Console.

3.20 Web Service Extension Restriction List (WebSvcExtRestrictionList)

Specifies IIS 6.0 scripting extension restriction lists. This list includes ISAPIs and CGIs as well as their location, descriptive information, and a flag for determining whether the extension is on or off. These settings globally affect all web sites on the affected machine. This settings trump script mappings at the web site or Virtual directory level.

Discussion:

Removing unnecessary extensions can reduce the attack surface in the event of a compromise.

Remediation:

Only the required ISAPI extensions should be enabled. All other ISAPI extensions that are not used should be disabled. The "1" flag denotes an allowed extension and the "0" flag denotes a disallowed extension.

To make this change in IIS Admin tools:

1. Open the Internet Service Manager in the Microsoft Management Console.
2. Click the "Web Service Extensions"
3. Prohibit or deny as necessary, click properties for further configuration

4 - IIS Configuration (ASP .NET)

ASP.NET configuration files are XML files. The .NET Framework defines a set of elements that implement configuration settings, and the ASP.NET configuration schema contains elements that control how ASP.NET Web applications behave. Default configuration settings are specified in the Machine.config file located in the %SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ directory. Values are inherited by child sites and applications. If there is a configuration file in a child site or application, the inherited values do not appear, but can be overridden and are available to the configuration API. This section describes the ASP.NET configuration schema elements that can be configured in the Machine.config file and in application-specific Web.config files. (Description from MSDN Documentation)

ASP.NET settings will in most cases trump IIS settings. For example, Custom Errors pages defined in a web.config will override settings defined in the IIS MetaBase for the particular site. Furthermore settings in web.config files trump settings in machine.config files.

Below is a list of configuration settings which have been determined to have an impact on security

References: http://msdn2.microsoft.com/en-us/library/b5ysx397.aspx

4.1 SessionState

The SessionState element configures how and if persistent session information is stored (see also ASP.NET System.Web.Session namespace). Session information can be stored in process (InProc), on a dedicated server (StateServer), or via SQL Server (SQLServer).

Discussion:

Disabling the session state will prevent the application from being more vulnerable to session stealing attacks.

Remediation:

Disable the SessionState service if it is not used. If a SQL Server is used for storing session information the connection should use Integrate Authentication and credentials should not be present in the configuration file.

4.2 Authorization

Determine the appropriate Authorization settings
The Authorization element restricts access and forces a login.

Discussion:

If authorization is determined, the user will be automatically redirected to a page where they must submit their credentials.

Remediation:

To set a restricted folder is for authenticated and SSL access only, set "deny users="?". " To set unauthenticated users to view Virtual Directories, and they do not need to be secured with SSL, set allow users="*" .

4.3 Forms

Set Forms elements to secure settings.
The Forms element configures applications for forms-based authentication methods.

Discussion:

Setting the sliding expiration to false will protect against reduce risk in case the authentication token is hijacked. Setting a cookie with a short life time will provide an attacker a short amount of time to impersonate the user.

Remediation:

Make sure that forms authentication cookies are protected, and that the authentication cookie life time is reduced when SSL is not used. The authentication cookie should be protected over the network. Set slidingExpiration to “false” when SSL is not used if concerned about cross-site scripting attacks and cookie hijacking.

4.4 Authentication

Check the authentication mode
The Authentication element governs the application's authentication mechanism.

Discussion:

If authorization is determined, the user will be automatically be prompted to submit their credentials to access sensitive pages.

Remediation:

Check the mode attribute to see which authentication method is configured and which option is appropriate for the application. The following list breaks down authentication types:

1. **Windows Authentication:** Authentication is integrated into Windows to validate a user's identity. These credentials are relayed to clients when users supply a log on to Windows.
2. **No Authentication:** Users are automatically logged onto a system as anonymous or guest without being prompted for credentials.
3. **.NET Passport (Windows Live ID):** Credentials are checked using a Passport authentication ticket stored in a cookie on the user's machine.
4. **Forms:** Authentication is provided using native code and maintains an authentication token in a cookie or a URL. This is executed by creating a logon page that collects credentials and authenticates those credentials against code.

   ```
   authentication mode="[Windows|Forms|Passport|None"]
   ```

4.5 Compilation

Remove debug information.
The compilation element controls whether the compiler produces debug builds which include debug symbols.

Discussion:

Removing the debugging information will prevent extraneous information such as stack traces and exception messages from being sent to the user in the event of an error.

Remediation:

Set the compilation element to debug="false" to prevent the displaying of debugging information to users.

```
compilation debug="false" explicit="true" defaultLanguage="vb"
```

4.6 Custom Errors

Determine what page is being returned when an exception occurs
The customError element configures custom, generic error messages that will be returned to the client in the event of an application exception condition.

Discussion:

Enabling this property will send a generic message to the user in the event of an error and not leak information.

Remediation:

Set the mode of customErrors to "ON" and redirect to a custom error page.

```
customErrors mode="On" defaultRedirect="YourErrorPage.htm"
```

4.7 HTTPForbiddenHandler

Map unused extensions to HTTPForbiddenHandler .
Web requests for specific file extensions are processed by HTTP handlers.

Discussion:

HTTPForbiddenHandler will prevent the download of unused file types. If a client requests a path that ends with .asmx, ASP.NET returns a message that says, "This type of page is not served."

Remediation:

Unused extensions should be mapped to HTTPForbiddenHandler. Remote extensions, such as .soap, .rem, on internet facing web servers should be mapped to HTTPForbiddenHandler.

```
      add verb="*" path="*.asax" type="System.Web.HttpForbiddenHandler
```

4.8 HttpRunTime

Check the maximum size of maxRequestLength in the httpRunTime element
The httpRunTime element contains settings that configure how a .NET application handles a request. The maxRequestLength attribute determines the length of for an input stream buffering threshold. This size is denoted in KB, and can be used to prevent Denial of Service attacks.

Discussion:

HttpRunTime can prevent the uploading of very large files with maximum size of 4mb

Remediation:

Verify the value of maxRequestLength attribute on the httpRuntime element.

httpRuntime maxRequestLength="4096000"

4.9 Identity

Check whether impersonation is enabled.
The Identity property enables impersonation, which uses an access token provided by IIS that represents the authenticated caller. This means that the service with an authenticated user will execute every resource when a request is made. This can include the anonymous Internet user account if the application uses Forms authentication. If the application uses

Windows authentication, it may also be a Windows account that represents the original caller.

Discussion:

Setting the Identity property will set fixed identities for specific virtual directories by using the following setting

Remediation:

The recommended setting for this property is "TRUE."

identity impersonate="true"

4.10 MachineKey

The MachineKey setting ensures that a Forms authentication cookie is encrypted. The keys and algorithms used for cookie encryption are specified on the MachineKey element.

Discussion:

The MachineKey property ensures authentication encryption.

Remediation:

Set the validation element to SHA1 if the view state is enabled.

machineKey validationKey="AutoGenerate,IsolateApps"
decryptionKey="AutoGenerate,IsolateApps" validation="SHA1"

4.11 Pages

The Pages element specifies configuration information for ASP .NET pages.

Discussion:

The pages element allows for disabling page buffering, session state, or view state. It can also detect view state tampering.

Remediation:

To detect view state tampering, set the enableViewState property to "TRUE" and the enableViewStateMac property to "TRUE."

pages enableViewState="true" enableViewStateMac="true"

4.12 ProcessModel

Check credentials in the ProcessModel element.
The ProcessModel element defines a least-privileged account to be used in an ASP .NET process. These credentials are encrypted for custom accounts by using Aspnet_setreg.exe.

Discussion:

The principle of a non-privileged user is one that is running under least privilege, meaning they are non-admin users with limited functionality.

Remediation:

Do not store plain-text credentials in machine.config. Use Aspnet_setreg.exe utility to store encrypted credentials in the registry (see documentation for aspnet_setreg.exe command line tool for more information)

4.13 Trace

Check tracing debug information
Tracing enables trace log output for every page within an application.

Discussion:

Disabling tracing will reduce the amount of information leakage in the event of an error.

Remediation:

Do not enable tracing on production servers. This information assists an attacker to profile an application and probe for weak spots.

trace enabled="false"

4.14 Trust

Set the appropriate trust level.
The trust element sets the code access security trust level used to run ASP.NET Web applications and Web services. The trust element takes the following properties:
level="[Full|High|Medium|Low|Minimal]"

Discussion:

Setting the trust level element will ensure that the appropriate security level is used for applications and Web services.

Remediation:

Full trust should not be used. Set the trust level on the Trust attribute to Medium: level="MEDIUM"

Revision History

Original Version 0.9 April-July 2007 -- Editor Shyama Rose
Consensus updates 1.0 Aug 2007 -- Editor Shyama Rose