When this document is printed, the document needs to be stamped top and bottom with the appropriate classification.

VL05 - Checklist Report

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:
Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Checklist: IIS Web Site 5

Vulnerability Key: V0002268
STIG ID: WA000-WI030
Release Number: 4
Status: Active
Short Name: WA000-WI030
Long Name: The IUSR_machinename account has read access to the .inc files or their equivalent.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 17 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Owing to the nature of .inc files, which may contain sensitive logic and potentially reveal sensitive information about the architecture of the web server, it is vital that the end user not be able to access and examine code that is included in .inc files. When server side scripting is the preferred method, this is normally not a problem. Nonetheless, there are key files inherent to the process, which can contain information key to the logic, server structure and configuration of the entire application. .inc files are the include files for many .asp script files. If the correct file name is guessed or derived, their contents will

be displayed by a browser. The file must be guarded from prying eyes of the anonymous web user. If the site has named thier include files with the .asp extension, then the files will be processed as an .asp file, which by the nature of .asp, will prevent that code from being presented. If the files are named with the .inc extension, or equivilent, you do not have this advantage. Java Server Pages, jsp, is another example of a competing technology which the reviewer will also encounter, that are impacted by this issue. The sample principles outlined here will apply to inlcude files used with Java Server Pages. In addition, there are some additional files that need to be protected, which include the global.asa and global.asax files.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1
Guide to the Secure Configuration and Administration of Microsoft Internet Information

Checks: WA000-WI030 (Manual)

Using IIS Manager, navigate to the web site you are reviewing, right click and selectt properties.

Go to the Home Directory tab, select the Configuration button, then the Mappings tab.

Review the following extension to see if they are mapped to the asp.dll:

.asa
.asax
.inc

If these extension are mapped to the asp.dll or aspnet_isapi.dll, this would not be a finding and you can stop the check procedure here.

If they are not mapped to the asp.dll continue with the following procedure to determine if these files are protected via file permissions.

Start >> Search >> Files and Folders >> Search for instances of the following:

global.asa
global.asax
files with the .inc extension.

If the files are part of the directories for the web site you are reviewing, move to these files, if found, and right click on them to view their Properties.

NOTE: You can check using IIS Manager, to determine which directory is associated with the web site. Web Site properties, Home Directory tab.

Read permissions should not exist for the:

IUSR_machinename account (the anonymous web user).

If the IUSR_machinename account has read access to the global.asa, global.asax, or .inc files, and these extensions are not mapped to the asp.dll (see procedure at the top), this is a finding.

Vulnerability Key: V0002267
STIG ID: WA000-WI050
Release Number: 6
Status: Active
Short Name: WA000-WI050
Long Name: Unused and vulnerable script mappings in IIS are not removed or set to the 404.dll.

IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 17 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site 5 (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: IIS file extensions which require server-side processing, but which have been deemed vulnerable, include .htr, .htw, .ida, .idc, .idq, .printer, .shtml, .shtm, .bat, .cmd and .stm. Requests to these file types can exploit a stack buffer overflow weakness in the ism.dll, httpodbc.dll, and ssinc.dll. A widely available exploit exists which allows a malicious user to gain administrative access to Windows NT/Windows 2000 host servers. These mappings have been exploited by malicious users to gain privileged access to web servers.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)
Guide to the Secure Configuration and Administration of Microsoft Internet Information

Checks: WA000-WI050 IIS5 (Manual)

From Internet Servicer Manager>> Select the web site to be examined; select Properties option by right clicking; Select the Home Directory tab. On this menu page, select the Configuration button; then App Mappings Tab.

Check for the presence of the following:

.htr, .htw, .ida
.idc, .idq, .printer,
.shtml, .shtm, .stm
.bat, .cmd

If these script mappings are mapped to the 404.dll this satisfies the requirement.

If any of the above listed mappings exist and are not mapped to the 404.dll, this is a finding.

NOTE: This vulnerability can be documented locally with the IAM/IAO if the site has operational reasons for the use of particular script mappings. If the site has this documentation, this should be marked as Not a Finding.

Vulnerability Key: V0003963
STIG ID: WA000-WI070
Release Number: 4
Status: Active
Short Name: WA000-WI070
Long Name: Content Index Service indexes directories, other than web document directories.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 24 Oct 2003

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: Enabling indexing also facilitates directory traversal exploits. To reveal such information to a malicious user is potentially harmful. Such information and the contents of files listed are normally readable by the anonymous Web user, yet are not intended to be viewed as they often contain information relevant to the configuration and security of the Web service. The indexing service can be used to facilitate a search function for large Web sites.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1

Checks:

WA000-WI070 (Manual)

From Internet Services Manager:

>> Select web site to be examined. Select Properties option by right clicking. Select Home Directory tab.

In the dialog menus that appear, if the Indexing checkbox is selected, go to the Services from Administrative Tools in Control panel and check to see if the Indexing Service is installed. If it is, determine if the start mode is either “Automatic” or “Manual“.

If the Indexing checkbox is not checked or the indexing service is not installed or disabled, this is not a finding.

If the Indexing checkbox is checked and the service is either Manual or Automatic, use the following procedure to examine the directories to be indexed.

With the assistance of the web administrator and or SA use the Microsoft Management Console (MMC) to evaluate this catalog. Start >> Run >>mmc >> console >> add remove snap-in >> indexing service (add). Review the directories being indexed.

If this service is in use only the web content folders should be indexed. If you are not sure if it is a

web content folder, examine the Home Directory tab within the properties of the web site. This will indicate the path of the content for this web site.

If the Index Service is running and directories other than web content directories are being indexed, this is a finding.

Vulnerability Key: V0006755
STIG ID: WA000-WI090
Release Number: 3
Status: Active
Short Name: WA000-WI090
Long Name: Directory Browsing is not disabled.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: This ensures that your directory structure, filenames, and web publishing features are not accessible. Such information and the contents of files listed are normally readable by the anonymous web user, yet are not intended to be viewed as they often contain information relevant to the configuration and security of the web service. The Directory Browsing feature can be used to facilitate a directory traversal and subsequent directory traversal exploits.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1
Guide to the Secure Configuration and Administration of Microsoft Internet Information

Checks: WA000-WI090 (Manual)

Using IIS Manager:

Select the web site to be examined. Select the Properties option. Select the Home Directory tab.

In the window that appears, if the Directory Browsing checkbox is selected, Directory Browsing is enabled.

If the Directory Browsing feature is enabled this is a finding.

Vulnerability Key: V0006247
STIG ID: WA025
Release Number: 3
Status: Active
Short Name: WA025
Long Name: Web content classification or sensitivity level has not been documented by proper authorities and appropriate labeling in not present.
IA Controls: ECML-1 Marking and Labeling
Categories: 5.1 Device Labels for Classification
11.2 Dissemination
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: If the sensitivity level of the data on a web server is unknown a procedure must be in place to ascertain this sensitivity level. Once the sensitivity level is known it is the responsibility of the IAO or approving authority to document this level. This sensitivity level is defined as data that has or has not been reviewed and approved for release in accordance with DoD 5230.9. Provided the level of sensitivity is known the web server can be defined as either a private or public web server and security controls can be applied accordingly. A DoD private web server as defined by the Department of Defense Instruction 8520.2 states: E2.1.12. DoD Private Web Server. For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation. A DoD public web server is any DoD-owned, operated, or controlled web server providing access to information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). The existence of unlabeled classified content is a de facto security incident. Thus a classified web server must contain correctly labeled material. These classified markings must be present on each page that contains classified content.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Web Administrator

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5

WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9

Checks:

WA025 (Manual)

Interview the IAO or Web Master to determine whether documentation exists defining the sensitivity level of data published by the Web site. The reviewer should also randomly review a few pages from the web site, if is a classified web server, and evaluate if classification markings are utilized on the pages.

If the sensitivity level of the information for publication by the web server is not known and documented, this is a finding.

If the classified web site does not contain proper labeling of content, this is a finding.

Vulnerability Key: V0002239
STIG ID: WA030
Release Number: 8
Status: Active
Short Name: WA030
Long Name: Web content is not reviewed and approved by proper authorities prior to posting to a production web server.
IA Controls: DCPR-1 CM Process
Categories: 12.9 Documentation
Effective Date: 09 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The organization or activity that sponsors the web site will have web content responsibility. These persons will ensure that all information is kept current and that information and scripting placed on the web server is reviewed and approved by a configuration management authority. The organization or activity that sponsors the web site will have web content responsibility. These persons will ensure that all information is kept current and that information and scripting placed on the web server is reviewed and approved by a configuration management authority and as needed by the Public Affairs Officer (PAO). Likewise, the reviewer should verify that local policies have been developed to ensure that all information has been reviewed and approved for posting by the originating organization according to the DoD Web Site Administration Policies & Procedures, 25 November 1998 (updated 11 January 2002) available at http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_correctio November 1998.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Designated Approving Authority

Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1

Checks: WA030 (Manual)

Reviewer should verify that local policies have been developed to ensure that all information has been reviewed and approved as needed by the Public Affairs Officer (PAO) for posting.

Proposed Questions:

How often does content change on the web site?
When content changes, how is the new content approved for publication?
Is the approval process documented in a local SOP?
Is the approval process documented in email?
Is the approval process documented in any manner?

Exceptions: Web applications where this Vulnerability is not applicable include computer or CD-ROM based training (CBT), document management applications, search and query applications or web sites designed for collaboration. Such applications will contain a rule-based structure for the posting and maintenance of content. In such cases, the rules by which such a site operates constitutes the review and approval process outlined in this requirement.

Vulnerability Key: V0013614
STIG ID: WA032
Release Number: 2
Status: Active
Short Name: WA032
Long Name: The Web Manager will ensure all interactive (CGI) programs used on the web server are documented, to include the language used and aim of the program, and that documentation is provided to the IAO.
IA Controls: ECSD-1 Software Development Change Controls
Categories: 12.9 Documentation
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: CGI is a standard for interfacing external applications with information servers, such as HTTP or web servers. The definition of CGI as web-based applications is not to be confused with the more specific .cgi file extension. CGI applications can be written in most programming language. Common applications involve acquiring data via a web page and the browser, executing the CGI application, and returning customized web content. There is a possibility of compromising security when using CGI. CGI programs that are carelessly written can grant the malicious user as much access to the server as a privileged account. Documenting these programs will allow the site to maintain an inventory of the interactive programs so that rogue programs are not installed and run from the web server.

Documentable: No

Documentable

Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2

Checks: WA032 (Manual)

The Web Manager will ensure all CGI programs used on the web server are documented, to include the language used and aim of the program, and that documentation is provided to the IAO.

Proposed Questions:

Review the SOP that documents this process.
Ask to see an example of a documented program from the web server.

If the site cannot produce documentation that show they are maintaining documentation of interactive programs, this is a finding.

Vulnerability Key: V0002269
STIG ID: WA130
Release Number: 4
Status: Active
Short Name: WA130
Long Name: Scripts are not reviewed by a CCB or technical group and installation of scripts on the web server is not controlled.
IA Controls: ECSD-1 Software Development Change Controls
ECSD-2 Software Development Change Controls
Categories: 7.4 Testing
7.7 Code Validation
12.4 CM Process
Effective Date: 17 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: Interactive scripts is a powerful means for enhancing web site functionality. Scripts are often executable at the operating system level and frequently exercise control over fundamental system resources (i.e start and stop programs, write data to the server, alter and delete data). A variety of scripting languages, middleware, is available for this purpose. Typically, this middleware involves the use of an interpreter. The opportunity for a malicious user to exploit poorly designed or untested web scripts is significant and has proven to be a leading cause of server compromises. This would apply to any operating system and any web server software in use. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.1, Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WA130 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine whether or not scripts are reviewed and evaluated for security issues prior to being installed on a production web server.

Another concern is that developers are allowed to directly install their own scripts onto the server. This should not be permitted. All interactive programs used on the web server should also be documented, to include the language used and aim of the program, and that documentation is provided to the IAO.

Proposed Questions:

Who approves the installation of scripts on the production web server?
What is the process for posting interactive programs to the web site?
Where is the list of documented interactive programs maintained?
Is the approval process documented in email? or in any manner?

If the scripts used on the web server are not filtered through a review process or CCB before posing and are not documented, this is a finding.

Exceptions: Web applications where this vulnerability is not applicable include computer or CD-ROM based training CBT), document management applications, search and query applications or web sites designed for collaboration. Such applications will contain a rule-based structure for the posting and maintenance of content.

Vulnerability Key: V0013615
STIG ID: WA150
Release Number: 1
Status: Active
Short Name: WA150
Long Name: Web applications or servers, which require restriction by user ID and password, do not require web users to have a user ID and password that provide access only to the web content.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 1.3 Identity Management
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Some web-based applications utilize the use of user IDs and passwords. In some cases these passwords are OS accounts and provide remote user access to other applications or databases. In this situation, the OS password policy applies. In other instances, the user ID and password scheme is determined by the application. In this case, the application's documentation should detail the policy to be followed to add users and select or change passwords. In cases where a Lightweight Directory Access Protocol (LDAP) server is used for authentication, the procedures for the web server suite should detail the web site's password policy. A process for changing the forgotten password should be followed. Password policies to include password strength will comply with the appropriate operating system STIG.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility:

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.6

Checks: WA150 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if web applications or servers, which require restriction by user ID and password, require web users to have a user ID and password that provide access only to the web content. The intent is to ensure that web users do not have access beyond what is necessary to access the web site.

Proposed Questions:

Ask them to provide documentation to show how userids are assigned. This should detail how regular users and administrative users are assigned accounts.

If the site is using OS accounts for web access, ask how the accounts are segregated. Is this done with groups, permissions, etc.?

If the site cannot explain to your satisfaction that they have a process for ensuring web userids are used to access only web content, then this is a finding.

Vulnerability Key: V0002240
STIG ID: WG110
Release Number: 5
Status: Active
Short Name: WG110
Long Name: The number of simultaneous requests is not limited for this web site.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 13.6 Denial of Service
Effective Date: 09 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: This check verifies that the web site is not configured to permit an unlimited number of HTTP requests. When this parameter is set to unlimited this facilitates a denial of service attack.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4
Guide to the Secure Configuration and Administration of Microsoft Internet Information

Checks:

WG110 - IIS 6 (Manual)

From the Internet Services Manager Select the web site to be examined; Select Performance tab; in dialog menus which appear, the choice Connections Unlimited is NOT to be selected.

WG110 - IIS 5 (Manual)

From the Internet Services Manager Select the web site to be examined; Select Web Site tab; under connections, the choice Unlimited is NOT to be selected.

Vulnerability Key: V0006531
STIG ID: WG140
Release Number: 2
Status: Active
Short Name: WG140
Long Name: A private web server does not require subscriber certificates, issued from any DoD authorized Certificate Authority as an access control mechanism for web users.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑

Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: The use of userids and passwords may lead to compromise of the userid and password, thus providing access to unauthorized individuals. Stronger authentication mechanisms will reduce this risk by providing additional factors of authentication before access is granted to the system. Per the DoDI 8520.2 all private web servers are required to request a subscriber certificate issued from a DoD authorized Certificate Authority for authentication to access DoD private web sites.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks: WG140 - IIS (Manual)
Using Microsoft Internet Information Server

>> Internet Service Manager >> Select web site to be examined;
Select Properties option by right clicking;
Select the Directory Security tab.

In Secure Communications area. “Require Secure Channel when accessing this resource” and “Require client certificates” must be checked.

If these are not checked, this is a finding.

NOTE: The DODI 8520.2 requires this for both NIPRNet and SIPRNet, but at this point, this should only be marked as a finding for NIPRNet web sites.

Vulnerability Key: V0013672
STIG ID: WG145
Release Number: 2
Status: Active
Short Name: WG145
Long Name: The private web server does not use an approved DoD certificate validation process.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: Without the use of a certificate validation process, the site is vulnerable to accepting certificates that have expired or have been revoked. This would allow unauthorized individuals access to the web server. This also defeats the purpose of the multi-factor authentication provided by the PKI process.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5

Checks:

WG145 - IIS6 (Manual)

This check will verify that the IIS web server is configured to use a certificate revocation list (CRL) to validate the user certificate that is being presented for access to the web site.

Using notepad, open the IIS metabase and search for the CertCheckMode key. If the value of this key is equal to 1, this is a finding.

NOTE: The value for this parameter defaults to 0, which means the CRL checking is enabled. So, if the web site you are reviewing is missing this parameter, this would not be a finding.

NOTE: If the property exists in both the server location, w3svc/cercheckmode, and at the site level, w3svc/x/certcheckmode, the value at the site will override the value at the server level. So, in this case, if the server is set to 0, and the site is set to 1, it would be a finding for the site you are reviewing.

The IIS metabase, by default, can be found in %systemroot%\system32\inetsrv\metabase.xml

Once the metabase is opened in notepad, do a search for the "CertCheckMode" key. To make sure you are looking at the parameters for the correct web site, a "ServerComment" key should be visible a few lines after the CertCheckMode key, and the comment in quotes should be the name of the web site you are reviewing.

WG145 - IIS5 (Manual)

This check will verify that the IIS web server is configured to use a certificate revocation list (CRL) to validate the user certificate that is being presented for access to the web site.

Open a command prompt and navigate to the inetpub\adminscripts directory.

From there, enter the following command:

Adsutil.vbs get w3svc/certcheckmode

If the command returns a message the parameter is not set, execute the following command, as the parameter may be set at the site level.

adsutil.vbs get w3svc/1/certcheckmode

The utility will either return an error message that the property does not exist, if this is the case, this is not a finding as the default value is to enable CRL checking, which is a value of 0.

It may also return either a 0 or 1 value if the property exists.

If it is set to 1, this is a finding.

If it is set to 0, this is not a finding.

NOTE: You may have to put cscript in front of the command. "cscript adsutil.vbs get w3svc/x/certcheckmode".

If the directory does not exist, you can search the system for the adsutil.vbs file.

If the property exists in both the server location, w3svc/cercheckmode, and at the site level, w3svc/x/certcheckmode, the value at the site will override the value at the server level. So, in this case, if the server is set to 0, and the site is set to 1, it would be a finding for the site you are

reviewing.

To make sure you are looking at the parameters for the correct web site, you can query for the "ServerComment" property using the following command:

adsutil.vbs get w3svc/1/servercomment

It should return something similar to "Default Web Site" or whatever the web site was named. This is visible in the Internet Services Manager Window under the list of web sites.

The IIS metabase, by default, can be found in %systemroot%\system32\inetsrv\metabase.bin.

Vulnerability Key: V0002245
STIG ID: WG170
Release Number: 5
Status: Active
Short Name: WG170
Long Name: Each readable web document directory does not contain either a default, home, index or equivalent file.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The goal is to completely control the web users experience in navigating any portion of the web document root directories. Ensuring all web content directories have at least the equivalent of an index.html file is a significant factor to accomplish this end. Also, enumeration techniques, such as url parameter manipulation, rely upon being able to obtain information about the web server's directory structure by locating directories with default pages. This practice helps ensure that the anonymous web user will not obtain directory browsing information nor an error message that reveals the server type and version.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG170 - IIS (Manual)

From the Internet Services Manager >> Select web site to be examined; select Properties option by right clicking; Select the Documents tab. The check box, Enable Default Document must be checked and there must be at least one file name present in the text box on this screen.

This applies to the document root and any virtual directories associated with this web site.

In a navigator window locate the Home Directory for the web site. Sample several subdirectories looking for a default file type as defined by the Documents tab in the ISM.

If the web site or virtual directory does not have a default page defined or if the default page does not exist, this is a finding.

NOTE: If the site has directory browsing disabled for the site or virtual directory, this would not be a finding if a default page does not exist.

Vulnerability Key: V0003333
STIG ID: WG205
Release Number: 5
Status: Active
Short Name: WG205
Long Name: The web document (home) directory is not in a separate partition from the web servers system files.
IA Controls: DCPA-1 Partitioning the Application
Categories: 2.2 Least Privilege
Effective Date: 05 Dec 2002

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Web content is accessible to the anonymous web user. For such an account to have access to system files of any type is a major security risk that is entirely avoidable. To obtain such access is the goal of directory traversal and URL manipulation vulnerabilities. To facilitate such access by mis-configuring the web document (home) directory is a serious error. In addition, having the path on the same drive as the system folder compounds potential attacks such as drive space exhaustion.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG205 - IIS (Manual)

Using the Internet Information Services Console, locate the web site being reviewed. Select this web site and right click on it, then select its Properties. When the menu screens appear, select the Home Directory tab. Make a note on the checklist sheet of the path to the web site's home directory.

This is a finding if:

- The directory is on the same partition as the operating systems root directory

or

- The directory is a child directory to the web application directory.

Vulnerability Key: V0002226
STIG ID: WG210
Release Number: 4
Status: Active
Short Name: WG210
Long Name: Web content directories anonymously shared via a network share.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Such sharing is a security risk when a web server is involved. Users accessing the share anonymously could experience privileged access to the content of such directories. Network sharable directories expose those directories and their contents to unnecessary access. Any unnecessary exposure increases the risk that someone could exploit that access and either compromises the web content or cause web server performance problems. NIST Guidelines for Securing Public Web Servers (par. 8.6 pg. 75, a principle reference for this document) states "Do not mount any file shares on the internal network from the Web server or vice versa". The presence of shares is indicative of a remote management solution or a development server. Alternatives to shares are a secure ftp products or related remote admin tools.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sections 3.7

Checks: WG210 - IIS (Manual)

Move to the %systemroot%\system32\inetsrv\ directory and examine the properties of this directory. Sharing should not be selected

Using the Internet Information Services Console, locate the web site being reviewed. Select this web site and right click on it, then select its Properties. When the menu screens appear, select the Home Directory tab. Make a note on the checklist sheet of the path to the web site's home directory. Administrative shares are not exempt from this requirement.

Using Explorer, locate the path identified above. Right click on the directory to be examined. Select Properties; Select the "Sharing" tab. If the "Do not share this folder" is not selected, this is a finding.

Navigate to the "Web Sharing" tab, select the web site you are reviewing from the pull down menu. The "Share this folder" can be selected, and will be in most cases if the web site is readable.

The following entry could be present in the list:

"/"

If the web site is readable, the above entry will be in the list and is acceptable and should not be marked as a finding.

If there are any other aliases in the list, this is a finding.

Note: In the case of a storage area network or file storage network, where partitions on the storage device are dedicated to a front end /back end web services, the additional partitions will be mapped to the correct file storage network partition in the web server configuration. This can apply to both web content and web scripts.

NOTE: The presence of operating system shares on the web server is not an issue as long as the shares are not part of the web content directories. The use of shares to move content from one environment to another is permitted if the following conditions are met: they are approved by the IAM/IAO, the shares are restricted to only allow administrators write access, the use of the shares does not bypass the sites approval process for posting new content to the web server, and Developers are only permitted read access to these directories.

Vulnerability Key: V0002249
STIG ID: WG230
Release Number: 4
Status: Active
Short Name: WG230
Long Name: Web server administration is not performed over a secure path or at the console.
IA Controls: EBRU-1 Remote Access for User Functions
Categories: 8.1 Encrypted Data in Transit
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Logging in to a web server via a telnet session or using http or ftp in order to perform updates and maintenance is a major risk. In all such cases, userids and passwords are passed in the plain text. Acquiring such account information over a network is routinely accomplished and made all the worse by the fact that the account information so obtained is for privileged users. A secure shell service or https needs to be installed and in use for these purposes. Another alternative is to administer the web server from the console, which implies physical access to the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.5

Checks:

WG230 - IIS (Manual)

For a standalone member server administration could be accomplished securely via the MMC at the host console. It is recommended to limit any server administration to the local host using the MMC or ISM.

If the HTML version of the ISM or the HTTP Administration Server is used, it must be used with SSL enabled. The HTML version, however, can be used but is not recommended. If this option is used verify that SSL/TLS is used.

Using Internet Services Manager>> Select web site to be examined; Select the Properties of the web site in question >>Select Web Site Tab >> Note the entry for SSL Port. (i.e. 443)

Server administration could be accomplished via the MMC in a domain environment. This is performed by creating a remote MMC session with the target computer. User authentication relys on the host domain environment. Only Admiinistrators or Web Admins should have access to this resource.

Options for remote Terminal Windows sessions: Select START >> Programs >>look for F-Secure or equivalent program. Some versions of Windows compatible SSH are F-Secure SSH Tunnel, SecureCRT, NT sshd, and Tera Term with TTSSH.

Vulnerability Key: V0013686
STIG ID: WG235
Release Number: 1
Status: Active
Short Name: WG235
Long Name: Remote authors or content providers are able to upload files to the DocumentRoot directory without the use of a secure encrypted logon and secure encrypted connection.
IA Controls: EBRU-1 Remote Access for User Functions
Categories: 8.1 Encrypted Data in Transit
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable Not Reviewed	Comments:

☐	

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Logging in to a web server via a telnet session or using http or ftp in order to upload documents to the web site is a risk if proper encryption is not utilized to protect the data being transmitted. A secure shell service or https needs to be installed and in use for these purposes.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.6

Checks:

WG235 (Manual)

Query the SA to determine if there is a process for the uploading of files to the web site. This process should include the requirement for the use of a secure encrypted logon and secure encrypted connection.

NOTE: See results from WG230 for data that will assist in the validation of this vulnerability.

If the remote users are uploading files without utilizing approved encryption methods , this is finding.

Vulnerability Key: V0002250
STIG ID: WG240
Release Number: 5
Status: Active
Short Name: WG240
Long Name: Logs of web server access and errors are not established and maintained.
IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting
Categories: 10.2 Content Configuration
Effective Date: 10 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality

	I - Mission Critical	II - Mission Support	III - Administrative
Classified			

Grid:

	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are reported in the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Without these log files, SAs and Web Managers are seriously hindered in their effort to respond appropriately to suspicious or criminal actions targeted at the web site. Message board and collaboration servers also need to log SMTP activity, JavaScript chat, uploads, errors, activity, and all HTTP requests.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1 and Section 5.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG240 - Generic (Manual)

Query the SA to determine what the process is for the collection of web logs. This should include the logging of any third party add-on components to the web server.

Proposed Questions:

Ask to see the log files that have been collected.
How often are the log files archived?
What is the retention period for these log files?

The purpose is to see if log files exist and are available for the web site.

If web log files are not being maintained, this is a finding.

Vulnerability Key: V0013688
STIG ID: WG242
Release Number: 2
Status: Active
Short Name: WG242
Long Name: Log file data does not include the required data elements.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.2 Content Configuration
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are reported in the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Without these log files, SAs and Web Managers are seriously hindered in their effort to respond appropriately to suspicious or criminal actions targeted at the web site.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks: WG242 - IIS (Manual)

To verify the log settings:

Start >> Programs >> Administrative Tools >> Internet Services Manager >> Select Website to view properties >> Web Site Tab >>

Logging enabled must be checked, then select Advanced button.

Properties >> General Logging Properties provides the location of the log files.

Properties >> Extended Logging Properties. Items to be checked are:

Date, Time, Client IP Address, User Name, Method, URI Query, Http Protocol Status and Referrer

If the configuration of the log files does not meet the above configuration, this is a finding.

Vulnerability Key: V0002252
STIG ID: WG250
Release Number: 3
Status: Active
Short Name: WG250
Long Name: Users other than from the Auditors group have greater than read access to log files.
IA Controls: ECTP-1 Audit Trail Protection
Categories: 2.2 Least Privilege
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC /

	I - Mission Critical	II - Mission Support	III - Administrative

Confidentiality Grid:				
	Classified	☑	☑	☑
	Sensitive	☑	☑	☑
	Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. To ensure the integrity of the log files and protect the SA and Web Manager from a conflict of interest related to the maintenance of these files, only the members of the Auditors group will be granted permissions to move, copy and delete these files in the course of their duties related to the archiving of these files.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks: WG250 - IIS (Manual)

To determine the settings:

Start >> Programs >> Administrative Tools >> Internet Services Manager >>
Select Website to view properties >> Web Site Tab >> Properties >> General Logging Properties provides the location of the log files

After locating the logs, use the Windows Explorer to move to these files and examine their properties:

Properties >> Security >> Permissions. Permissions greater than Read, Execute should be noted for only the System and the Auditors Group.

If the SA, Web Manager or users other than the Auditors group have greater than read access to the log files, this is a finding.

Vulnerability Key: V0013689
STIG ID: WG255
Release Number: 2
Status: Active
Short Name: WG255
Long Name: Access to the web server log files is not restricted to Administrators, the user assigned to run the web server software, Web Manager, and Auditors.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: A major tool in exploring the web site use, attempted use, unusual conditions and problems are the access and error logs. In the event of a security incident, these logs can provide the SA and Web Manager with valuable information. Because of the information that is captured in the logs, it is critical that only authorized individuals have access to the logs.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks:

WG255 - IIS (Manual)

To determine the settings:

Start >> Programs >> Administrative Tools >> Internet Services Manager >> Select Website to view properties >> Web Site Tab >> Properties >> General Logging Properties provides the location of the log files

After locating the logs, use the Windows Explorer to move to these files and examine their properties:

Properties >> Security >> Permissions.

If anyone other than the Auditors, Administrators, Web Managers, System, and the service used to run the web server has read access to the log files, this is a finding.

Vulnerability Key: V0002254
STIG ID: WG260
Release Number: 4
Status: Active
Short Name: WG260
Long Name: Web sites still under development exist on a production server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 11.2 Dissemination
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑

Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: In the case of a production web server, areas for content development and testing will not exist, as this type of content is only permissible on a development web site. The process of developing on a functional production web site entails a degree of trial and error and repeated testing. This process is often accomplished in an environment where debugging, sequencing and formatting of content are the main goals. The opportunity for a malicious user to obtain files that reveal business logic and login schemes is high in this situation. The existence of such immature content on a web server represents a significant security risk that is totally avoidable.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.8
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG260 (Manual)

The reviewer should query the IAO, SA and Web Manager to find out if development web sites are being housed on production web servers.

Definition: A production web server is any web server connected to a production network, regardless of its role.

Proposed Questions:

Do you have development sites on your production web server?
What is your process to get development web sites / content posted to the production server?
Do you use under construction notices on production web pages?

You can also do a manual check or navigation of the web site via a browser could be used to confirm the information provided from interviewing the web staff. Graphics or text which proclaim Under Construction or Under Development are frequently used to mark folders or directories in that status.

If under construction or development web content is discovered on the production web server, this is a finding.

Vulnerability Key: V0006373
STIG ID: WG265
Release Number: 7
Status: Active
Short Name: WG265
Long Name: The approved DoD banner page is not in place on the web server.
IA Controls: ECWM-1 Warning Message
Categories: 11.6 Warning Banners
Effective Date: 29 Jun 2005

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category III

Vulnerability Discussion: A consent banner will be in place to make prospective entrants aware that the web site they are about to enter is a DoD web site and their activity is subject to monitoring. The May 9, 2008 Policy on Use of Department of Defense (DoD) Information SystemsStandard Consent Banner and User Agreement, establishes interim policy on the use of DoD information systems. It requires the use of a standard Notice and Consent Banner and standard text to be included in user agreements. The requirement for the banner is for web sites with security and access controls. These are restricted and not publicly accessible. If the web site does not require authentication / authorization for use, then the banner does not need to be present.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG265 (Manual)

The reviewer should query the IAO, SA and Web Manager on this point.

A manual check of the document root directory for a banner page file (such as banner.html) or navigation to the web site via a browser can be used to confirm the information provided from interviewing the web staff.

The following banner page must be in place:

“You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.”

Option 2: If your system cannot meet the character limits to store this amount of text in the banner, the following is another option for the warning banner:

"I've read & consent to terms in IS user agreem't."

NOTE: This has to be displayed only once when the individual enters the site and not for each page.

If the access controlled web site does not display this banner page before entry, this is a finding.

NOTE: If the web site does not require authentication / authorization for use, then the banner does not need to be present.

Vulnerability Key: V0002258
STIG ID: WG290
Release Number: 4
Status: Active
Short Name: WG290
Long Name: The web client account access to the content and scripts directories is not limited to read and execute.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category I

Vulnerability Discussion: Excessive permissions for the anonymous web user account are one of the most common faults contributing to the compromise of a web server. If this user is able to upload and execute files on the web server, the organization or owner of the server will no longer have control of the asset.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG290 - IIS (Manual)

Determine the web client account (anonymous account) for the web server software that is installed.

For the web content and script directories, determine the permission for the web client account. Permissions for this account should be read and execute or more restrictive.

Verify if the IUSR_computername and IWAM_computername accounts are in the Guests Group or

as authenticated users. Then examine the permission of these accounts on the document root directory.

If the web client account access to the content and scripts directories is not limited to read and execute, this is a finding.

If the Microsoft 'everyone' account has access to these directories, this is a finding.

Vulnerability Key: V0002260
STIG ID: WG310
Release Number: 4
Status: Active
Short Name: WG310
Long Name: A Private web server responds to requests from public search engines.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: Search engines are constantly at work on the Internet. Search engines are augmented by agents, often referred to as spiders or bots, that endeavor to capture and catalog web site content. In turn, these search engines make the content they obtain and catalog available to any public web user. Such information in the public domain defeats the purpose of a Limited or Certificate-based web server, provides information to those not authorized access to the web site, and could provide clues of the sites architecture to malicious parties.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG310 - IIS (Manual)

Query the SA to determine what type of restriction from public search engines is in place. This can be accomplished in several ways.

In the Home directory check for a file named robots.txt which contains at least the following content:

User-agent: *
Disallow: /

Note: The robots.txt file must be placed in the document root directory. Additional restrictions can be stated in the robots.txt file. The above example will disallow access to all directories in the document root directory.

The location of the document root can be found by using Internet Service Manager and navigating to the web site you are reviewing. Choose the Home Directory tab and note the directory for the web site.

Also, if other restrictions are in place to limit access to the web site, this meets the requirement. You can view these restrictions using Internet Service Manager. Some examples:

Navigate to the web site you are reviewing, examine the properties, and from the Directory Security tab, review the Anonymous access and authentication control button to determine if controls are in place to prevent anonymous access.

In addition, you can examine the IP address and domain name restrictions button to determine if access to the web site is limited by IP or domain. The restriction needs to be specific, and not just at the root domain level. For example, if only .com is blocked, this would still require a robots.txt file in the Home Directory.

If no means of restriction is in place (e.g. userid and password, domain or IP restriction, user PKI certificate) or a robots.txt file is not in use, this is finding.

NOTES: It is recommended to to do both. Also, this applies to both SIPRNet and NIPRNet web servers.

Vulnerability Key: V0002262
STIG ID: WG340
Release Number: 5
Status: Active
Short Name: WG340
Long Name: A Private web server is not using TLS.
IA Controls: ECCT-1 Encryption for Confidentiality (Data in Transit)
ECCT-2 Encryption for Confidentiality (Data in Transit)
Categories: 1.2 PKI
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)
Policy: All Policies
MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II
Vulnerability Discussion: SSL/TLS encryption is a required security setting for a private web server. This check precludes the possibility that a valid certificate has been obtained, but SSL/TLS has not been activated or is not

being used. Transactions encrypted with trusted certificates are necessary when the information being transferred is not intended to be accessed by all parties on the network. To the extent that this standard applies, this check is valid for the SIPRNet also. In addition, the use of current technologies will lessen the risk of data exposure due to limitations in the encryption that is being utilized. The minimum standard is SSL V3.1 / TLS 1.0.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks: WG340 - IIS (Manual)

From the Internet Service Manager (this selection starts the Microsoft Management Console, MMC)

>> Select web site to be examined; Select the Properties of the web site in question >> Select Web Site Tab >> Note the entry for SSL Port. (i.e. 443)

Also examine the Directory Security tab and choose the Edit button in teh Secure Communications section. Determine if the Require secure channel (SSL) is selected and also if 128-bit encryption is required.

If the site does not require SSL and 128-bit encryption, this is a finding.

If the site requires SSL and 128-bit encryption, then the version of SSL also needs to be verified.

The following registry keys need to exist and be set to not allow anything lower than SSL V3.1 / TLS. This can be accomplished by ensuring the following value exists in each of the keys:

Enabled REG_DWORD 0

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\PCT 1.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\PCT 1.0\Server

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Server

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Server

If these keys are not set to a DWORD value of 0, this is a finding.

If the keys do not contain the value "Enabled", this would also be a finding.

The keys for TLS 1.0 do not require the Enabled value to be present, but if it is, it needs to be set to REG_DWORD 1, to enable SSL V3.1 / TLS.

NOTE: In some cases the web servers are configured in an environment to support load balancing. This configuration most likly utilizes a content switch to contol traffic to the various web servers. In this situration, the SSL certificated for the web sites may be installed on the content switch vs, the individual web sites. This solution is acceptable as long as the web servers are isolated from the general population LAN. We don't want users to have the ability to bypass the content switch to access the web sites.

Vulnerability Key: V0013694
STIG ID: WG342
Release Number: 2
Status: Active
Short Name: WG342
Long Name: Public web servers that use SSL do not use the correct version to provide encrypted sessions.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 1.2 PKI
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☐	☐	☐
Sensitive	☐	☐	☐
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Public web servers do not require the use of SSL certificates but if the web server is uitilzing a server based certificate it needs to meet the minimum standards, which is SSL V3.1 / TLS 1.0. The use of lesser or outdated technologies can increase the chance of data being exposed due to limitations in the encryption that is being utilized. Transactions encrypted with trusted certificates are necessary when the information being transferred is not intended to be accessed by all parties on the network. To the extent that this standard applies, this check is valid for the SIPRNet also.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13

Checks: WG32 - IIS (Manual)

From the Internet Service Manager (this selection starts the Microsoft Management Console, MMC)

Examine the Directory Security tab and choose the Edit button in teh Secure Communications section. Determine if the Require secure channel (SSL) is selected and also if 128-bit encryption is required.

If the site does not require SSL and 128-bit encryption, this is not a finding.

If the site requires SSL and 128-bit encryption, then the version of SSL also needs to be verified.

The following registry keys need to exist and be set to not allow anything lower than SSL V3.1 / TLS. This can be accomplished by ensuring the following value exists in each of the keys:

Enabled REG_DWORD 0

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\PCT 1.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\PCT 1.0\Server

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Server

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Client

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Server

If these keys are not set to a DWORD value of 0, this is a finding.

If the keys do not contain the value "Enabled", this would also be a finding.

The keys for TLS 1.0 do not require the Enabled value to be present, but if it is, it needs to be set to REG_DWORD 1, to enable SSL V3.1 / TLS.

Vulnerability Key: V0002263
STIG ID: WG350
Release Number: 3
Status: Active
Short Name: WG350
Long Name: A private web server that executes a web application does not have a DoD Certificate.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: This check verifies that DoD is the sites CA. The certificate is actually a DoD issued server certificate used by the organization being reviewed. This is used to verify the authenticity of the web site to the user. If the certificate is not for the server (Certificate belongs to), if the certificate is not issued by DoD (Certificate was issued by), or if the current date is not included in the valid date (Certificate is valid from), then there is no assurance that the use of the Certificate is valid. The entire purpose of using a certificate is therefore compromised.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.12
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks: WG350 (Manual)

Open browser window and browse to the appropriate site. Before entry to the site you should be presented with the servers DOD PKI credentials. Review these credentials for authenticity.

Find an entry which cites:

Issuer:
CN = DOD CLASS 3 CA-3
OU = PKI
OU = DoD
O = U.S. Government
C = US

NOTE: The "InstallRoot3.0_SAG" document, which is included on the SRR CD, has a complete list of DoD certificates.

If the server is running as a public web server this finding should be Not Applicable.

NOTE: In some cases the web servers are configured in an environment to support load balancing. This configuration most likly utilizes a content switch to contol traffic to the various web servers. In this situration, the SSL certificated for the web sites may be installed on the content switch vs, the individual web sites. This solution is acceptable as long as the web servers are isolated from the general population LAN. We don't want users to have the ability to bypass the content switch to access the web sites.

Vulnerability Key: V0013620
STIG ID: WG355
Release Number: 2
Status: Active
Short Name: WG355
Long Name: A private web server's list of CAs considered trusted is not limited to those with a trust hierarchy that leads to the DoD PKI Root CA or to an approved External Certificate Authority (ECA) or are required for the server to function.
IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards
Categories: 1.2 PKI
Effective Date: 27 Apr 2007

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality

	I - Mission Critical	II - Mission Support	III - Administrative

Grid:

Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☐	☐	☐

Severity: Category II

Vulnerability Discussion: A PKI certificate is a digital identifier that establishes the identity of an individual or a platform. A server that has a certificate provides users with third-party confirmation of authenticity. Most web browsers perform server authentication automatically; the user is notified only if the authentication fails. The authentication process between the server and the client is performed using the SSL/TLS protocol. Digital certificates are authenticated, issued, and managed by a trusted Certification Authority (CA). The use of a trusted certificate validation hierarchy is crucial to the ability to control access to your server and prevent unauthorized access. This hierarchy needs to lead to the DoD PKI Root CA or to an approved External Certificate Authority (ECA) or are required for the server to function.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.12.1

Checks: WG355 - IIS (Manual)

The reviewer will need to have the SA or Web Manager show the list of CA's the server is trusting to authenticate users.

NOTE: There are non DoD roots that must be on the server in order for it to function. Some applications, such as anti-virus programs, require root CAs to function.

From the IIS Management Console, Right Click on the Web Site you are reviewing. Then Select Properties, then the Directory Security tab. Under the Secure communications, select Edit, then if the Enable certificate trust list is checked, select edit. You will see prompt for the certificate trust list wizard, select next to be presented with the list of trusted CAs. If there are trusted CAs in this list that are not DoD, this is a finding.

If the Enable certificate trust list is not checked, this is not a finding.

The PKE InstallRoot 3.0 System Administrator Guide (SAG), dated 9 Nov 2006, contains a complete list of DoD, ECA, and IECA CAs.

Vulnerability Key: V0002229
STIG ID: WG410
Release Number: 4
Status: Active
Short Name: WG410
Long Name: Interactive scripts do not have proper access controls.
IA Controls: ECLP-1 Least Privilege
Categories: 2.2 Least Privilege
Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: CGI scripts represents one of the most common and exploitable means of compromising a web server. By definition, CGI are executable by the operating system of the host server. While access control is provided via the web service, the execution of CGI programs is not otherwise limited unless the SA or Web Manager take specific measures. CGI programs can access and alter data files, launch other programs and use the network. CGI programs can be written in any available programming language. C, PERL, PHP, Javascript, VBScript and shell (sh, ksh, bash) are popular choices. CGI is a standard for interfacing external applications with information servers, such as HTTP or web servers. The definition of CGI as web-based applications is not to be confused with the more specific .cgi file extension. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances.

Documentable: Yes

Documentable Explanation: The Microsoft SharePoint product will require "Scripts and Executables" for functionality. This situation would be considered valid for a documentable status. In this case, the IAM/IAO will need to be able provide doucment evidence of the acceptance of this risk.

Potential Impacts: With Windows and IIS using .asp or .jsp files, the comparable directory is the Scripts directory. Security is enhanced with virtual directories because it adds another level of abstraction to the site, altering the way in which Internet users access the information. Read, Write, Directory Browsing, Scripts only, and Scripts and executables are IIS permissions, which can be applied to a virtual directory and all of the files and folders contained within it; Scripts permissions for the web client accounts should be the setting. Read permission allows a client to download files stored in a virtual directory or subdirectory. Only directories that contain information to be published or downloaded should have Read permission set. To prevent clients from downloading executable files or scripts that always contain sensitive information and application logic, these files will be located in separate directories without Write permission. Instead, these virtual directories should have Script only permission so web clients can run them. Only the Scripts setting should be used. Additional configuration checks for IIS using .asp files are noted below and covered as noted by this check. IIS: IUSR_machinename NTFS account permissions – Read and Execute Locate all but the default.asp or equivalent file in a separate directory (ies) IIS: Internet Services Manager Settings on Home Directory tab, Execute Permissions: Script

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks:

WG410 - IIS (Manual)

From the Microsoft Internet Information Server >> Internet Service Manager (this selection starts the Microsoft Management Console, MMC)

>> Select web site to be examined; select Properties option by right clicking; Select the Home Directory tab.

In the Application Settings section, Execute Permissions must state Scripts only.

From the configuration button, App Options tab, Enable Parent Paths must NOT be checked. **Recommend ASP default language = VBScript and ASP Server = 90 seconds.

NOTE: Parent Paths allows you to use '..' in calls to MapPath and the like. By default this option is enabled and should be disabled.

To disable this option go to the root of the Web site in question, right click select Properties | Home Directory | Configuration | App Options and uncheck Enable Parent Paths.

NOTE: You should verify these setting on virtual directories as well. The name of the tab for the virtual directories is "Virtual Directory". The configuration button may not be enabled if it is using the setting from the parent web site, if it is enabled, then you should validate the settings identified in the manual procedures.

If the web user or other group has read and write access to CGI scripts, or in IIS the execute

permissions and applications settings are not as noted above, this is a finding.

Vulnerability Key: V0002230
STIG ID: WG420
Release Number: 7
Status: Active
Short Name: WG420
Long Name: Backup interactive scripts are present on the system.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 2.2 Least Privilege
Effective Date: 01 Dec 1999

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: Copies of backup files will not execute on the server, but can be read by the anonymous user if special precautions are not taken. Such backup copies contain the same sensitive information as the actual script being executed and as such are useful to malicious users. Techniques and systems exist today which search web servers for such files and are able to exploit the information contained in them. Backup copies of files are automatically created by some text editors such as emacs and edit plus. The emacs editor will write a backup file with an extension ~ added to the name of the original file; edit plus will create a .bak file. Of course, this would imply the presence and use of development tools on the web server, a finding under WG130. Having backup scripts on the web server provides one more opportunity for malicious persons to view these scripts and use information found in them.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG420 - Windows (Manual)

Find on all hard drives *.bak, *.old, *.temp, *.tmp, *.backup, or ‘copy of..’

Once the files are found, the reviewer must determine if the files are in the document or home directory of the web sever.

If files with these extensions are in this directory this is a finding. If not the reviewer must make a determination as to the relationship said file or files has with the web server.

If the files are stored in a repository (not in the document root) as backups for the web server this is also a finding.

If the files have no relationship with web activity, such as a backup batch file for operating system utility, this is not a finding.

Vulnerability Key: V0002270
STIG ID: WG430
Release Number: 3
Status: Active
Short Name: WG430
Long Name: Anonymous FTP users can access interactive scripts.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 25 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: The directory containing the CGI scripts, or equivalent scripting files such as PERL or asp file, must not be accessible to anonymous users via FTP. This applies to all directories that contain scripts that can dynamically produce web pages in an interactive manner; that is based upon user provided input. Such scripts contain information that could be used to compromise a web service, access system resources or deface a web site.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG430 - Windows (Manual)

Locate the directory containing the CGI, PERL, ASP, JS or JSP scripts.

Using a right click on the web content directory and related scripts directory. Using the Properties Tab, examine the access rights for the scripts, cgi-bin, cgi-shl, scripts or equivalent directory. Anonymous ftp users must not have access to these directories.

If the CGI directory can be accessed by any group that does not require access; this is a finding.

Vulnerability Key: V0002272
STIG ID: WG460
Release Number: 3
Status: Active
Short Name: WG460
Long Name: PERL is being used without the taint option.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 7.2 Writing Secure Code
Effective Date: 25 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: Web Server AND Windows (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category II

Vulnerability Discussion: PERL (Practical Extraction and Report Language) is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. The language is often used in shell scripting and is intended to be practical, easy to use and efficient means of generating interactive web pages for the user. Unfortunately many widely available freeware PERL programs (scripts) are extremely insecure. This is most readily accomplished by a malicious user substituting input to a PERL script during a POST or GET operation. Consequently, the founders of PERL have developed a mechanism named taint that protects the system from malicious input sent from outside the program. When the data is tainted, it cannot be used in programs or functions such as eval(), system(), exec(), pipes, or popen(). The script will exit with a warning message. It is vital that if PERL is being used, the following line appear in the first line of PERL scripts: #!/usr/local/bin/perl –T

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 4.5

Checks: WG460 - Windows (Manual)

It is vital that if PERL is being used the following line appear in the first line of PERL scripts:

#!/usr/local/bin/perl –T

The reviewer will normally use Notepad to view the content of a PERL script. Normally the form method that calls the script will contain the –T switch.

CGI Scripts running on non-UNIX Servers typically do not recognize the magical #!/usr/local/bin/perl first line of the script. Instead, the web server knows what language to execute the server with because of an operating system or web server configuration variable.

For example, for IIS on Windows, you should change the association of Perl scripts to run with "taint mode on". A more reasonable way to get around the problem is by creating a second extension under Windows such as tcgi or tgi and associate it with taint mode Perl. Then, rename the scripts with the new extension to activate taint mode on them.

If the server is using PERL and scripts do not include a call to the taint option, this is a finding.

NOTE: This applies to PERL scripts that are used as part of the web server and not all PERL scripts that are on the system.

NOTE: If the mod_perl module is installed, and the directive “PerlTaintCheck on” in the httpd.conf is used this satisfies the requirement.

Vulnerability Key: V0002265
STIG ID: WG490
Release Number: 6
Status: Active
Short Name: WG490
Long Name: Java software installed on the web server is not limited to class files and the JAVA virtual machine.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 7.7 Code Validation
Effective Date: 11 May 2001

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	Comments:

Condition: IIS Web Site (Target: IIS Web Site 5)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

Severity: Category III

Vulnerability Discussion: From source code in a .java or .jpp file, the Java compiler produces a binary file with an extension of .class. The .java or .jpp file would therefore reveal sensitive information regarding an applications logic and permissions to resources on the server. By contrast the .class file, because it is intended to be machine independent, is referred to a bytecode. Bytecodes are run by the Java Virtual Machine, JVM, or Java Runtime Environment, JRE, via a browser configured to permit Java code.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Secton 4.7

Checks: WG490 (Manual)

Search the web content directory and scripts directory for Java code other than .class, . jre and .jvm. Executables such as java.exe, jre.exe, and jrew.exe are permitted; but .java and .jpp files are not allowed on a production web server.

The reviewer should check for .java files in the web content directory

Unix:

Search the web content directory and scripts directory for Java code file other than .class.

Use: find / -name *.java or find / -name *.jpp

Windows:

Search the web content directory and scripts directory for Java code file other than .class.

Use: Start [Right Click] >> Search *.java with “look in local hard drives”; find *.jpp with “look in local hard drives”

If Java code with a .java or .jpp extensions are found in the web content or scripts directories, this is a finding.

Vulnerability Count - 34