

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: Netscape Site

Vulnerability Key: V0002238

STIG ID: WA000-WN010

Release Number: 3

Status: Active

Short Name: WA000-WN010

Long Name: The termination timeout is not set to one (1) second.

IA Controls: DCBP-1 Best Security Practices

Categories: 13.6 Denial of Service

Effective Date: 09 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: When a server is turned off, it stops accepting new connections and waits for the outstanding or extant connections to complete. The time the server waits before terminating these outstanding connections is the timeout setting. If for whatever reason the decision is made to stop the web service, outstanding connections should be dropped within a second thereafter to achieve the aim of service termination.

Documentable: No

Documentable**Explanation:****Potential****Impacts:****Responsibility:** Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.2**Checks:** WA000-WN010 (Manual)

Locate the magnus.conf file; typically in the /netscape/server4/[hostname]/config directory.

Check the magnus.conf file; it should contain the line TerminateTimeout 1

Note: This is NOT the same parameter as the Connection Timeout in IIS and Apache. Also a value of 0 is permissible in meeting this requirement as it is more restrictive.

Vulnerability Key: V0002241**STIG ID:** WA000-WN020**Release Number:** 3**Status:** Active**Short Name:** WA000-WN020**Long Name:** For Netscape web servers, automatic directory indexing is not turned off.**IA Controls:** ECAN-1 Access for Need-to-Know**Categories:** 2.2 Least Privilege**Effective Date:** 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III**Vulnerability Discussion:** This ensures that your directory structure, filenames, and web publishing features are not accessible.

Enabling fancy 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.

Documentable: No**Documentable****Explanation:****Potential****Impacts:****Responsibility:** Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.2**Checks:** WA000-WN020 (Manual)

Using the Administrative Server from the Server Manager, choose server | choose Virtual Server

Class | select class to manage (choose "manage") | choose Content Management | Document Preferences. If Directory Indexing or Fancy Indexing is marked "on" 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 is not present.

IA Controls: ECML-1 Marking and Labeling

Categories: 5.1 Device Labels for Classification
11.2 Dissemination

Effective Date: 29 Jun 2005

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 it 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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_corrections 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies

--	--	--	--

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WG110 - Netscape (Manual)

In the magnus.conf file, locate the parameter RqThrottle. This parameter specifies the maximum number of simultaneous connections the web server can handle. The default value for this parameter is 512. Suitable values for RqThrottle range from 200 to 3000. In the case of Netscape, if RqThrottle is greater than 3000, this is a finding.

Administration Web screen:

Select web site to be reviewed choose Manage | Preferences tab | Performance Tuning | Maximum Simultaneous Requests is displayed.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Restrictions based upon domain name, such as .gov or .mil are commonly used. In some cases, restriction down to the ip address of the host attempting to access the server is possible. Access can also require the client requesting a connection to a web server to possess a userid and password. However, per the DODI 8520.2 all private web servers are required to request a valid DOD PKI user certificate for authentication to access DOD private web sites. The use of non-standard port numbers is not an accepted solution to limiting access to a web server, as elementary port scanning tools will quickly reveal http and https services running on non-standard ports.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** Web Administrator

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.5
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling

Checks: WG140 - Netscape (Manual)
With the assistance of the SA or Web Manager only:

from the Administration server select web site and Manage
from the left menu select Restrict Access
select to view ALC list
Select ACL to be reviewed
look for access restriction of user pki certificate required.

If DOD PKI User Certificates are not required for access to a DOD Private web server, then this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---------------	--------------------------	--------------------------	--------------------------

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 - Generic (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the web server is configured to utilize an approved DoD certificate validation process.

The Webmaster should be questioned to determine if a validation process is being utilized on the web server.

To validate this, the reviewer can ask the Webmaster to describe the validation process being used. They should be able to identify either a CRL process or the preferred method, the Robust Certificate Validation Service (RCVS) or OCSP.

If CRLs are being used, the SA should be able to identify how often the CRL is updated and the location from which the CRL is downloaded.

If the Webmaster cannot identify the type of validation process being used, this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 2.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG170 - Netscape (Manual)

From the Administrative Server, for each web site, determine the document root. Ensure that in this directory there is an index.html (or equivalent file) and perform the same check on any directories below the root document directory.

Using the Administrative Server from the Server Manager, choose server | choose Virtual Server Class | select class to manage (choose "manage") | choose Content Management | Primary Document Directory to find document root. Proceed to Document Preferences and view Index Filenames and Home Page/Index File information.

Windows: Using explorer proceed to the document root and inspect this directory for the appropriate file.

UNIX: From the command line proceed to the document root and inspect this directory for the appropriate file.

If any web document directory does not contain a default, home, index or equivalent file, this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies

MAC / Confidentiality	I - Mission Critical	II - Mission Support	III - Administrative

Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9
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: WG205 - Netscape (Manual)

From the Administrative Server, for each web site, determine the document root.

Using the Administrative Server from the Server Manager, choose server | choose Virtual Server Class | select class to manage (choose "manage") | choose Content Management | Primary Document Directory to find document root. This information can also be obtained from the magnus.conf file.

Confirm that this directory is not located on the systems root partition nor the web root directory; if it is this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)**Policy:** All Policies

MAC / Confidentiality	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Grid:	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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. Access control is a major factor in limiting damage. 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 compromise the web content or cause web server performance problems.

Documentable: No**Documentable****Explanation:****Potential****Impacts:**

Responsibility: System Administrator
Web Administrator

References:**Checks:** WG210 - Windows Netscape (Manual)

Using the Administrative Server from the Server Manager, choose server | choose Virtual Server Class | select class to manage (choose "manage") | choose Content Management | Primary Document Directory to find document root.

Using Explorer, locate the path identified above. Right click on the directory to be examined. Select Properties; Select the "Sharing" tab. If the "Shared As" or "Web Sharing" radio buttons are selected, this is a finding.

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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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. Access control is a major factor in limiting damage. 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 compromise the web content or cause web server performance problems.

Documentable: No**Documentable****Explanation:****Potential****Impacts:**

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sections 3.2 and 3.9

Checks: WG210 - Unix Netscape (Manual)

Locate the highest-level directory containing web content. Netscape: In the Administrative Server, locate the document root and make a note of this path on the checklist sheet.

Likely locations for the web server's root directory are:

Netscape: /opt/netscape/suitespot/ or /opt/netscape/server4/

Or the entry for the Server Root directory can be found in the magnus.conf file. For example:
ServerRoot /usr/lpp/internet/server_root

The command /usr/bin/share or /usr/sbin/share will display all the file systems which are exported.

Look in the /etc/exports, /etc/mnttab or /etc/dfs/sharetab file. This file lists the file systems that the server exports. Look for the paths identified above. If these paths are present in either one of these files, this is a finding.

If the path for the web server root directory is present in the /etc/exports file, this is a finding.

If these files contain the names of directories used for the web service or web content on another server, this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

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

Severity: Category II

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 3.3**Checks:** WG230 - Netscape Windows (Manual)
Select START >> Programs and 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.

The administrative server uses the SSL (https) protocol. Start this server and observe the url. If the url does not include https, this is a finding.

This does not apply if all administration is accomplished at the host console. If all administration is done via the server console, this is not a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

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 3.2**Checks:** WG230 - Netscape Unix (Manual)
Verify that some variety of SSH is running on the web server platform

Check for an ssh daemon, by querying the SA and Web Manager and use `ps -ef | grep ssh`

Netscape: The administrative server uses the https protocol. Start this server and observe the url.

If the url to the Netscape Administrative Server does not include https, this is a finding.

This does not apply if all administration is accomplished at the host console.

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

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 - Generic (Manual)

Query the SA to determine what the process is for the collection of web logs.

Following is an example of the items that should be logged:

Logging Properties. Items to be checked are: Date, Time, Client IP Address, User Name, Method, URI Query, Http Protocol Status and Referrer for the following events:

- Successful and unsuccessful attempts to access the web server software.
- Successful and unsuccessful attempts to access the web site.
- Successful and unsuccessful attempts to access the web application.

Proposed Questions:

Ask to see the log files that have been collected to determine if the required information is being 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 contain the correct data elements for the identified conditions.

If web log files do not contain the correct data elements, 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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:****Checks:** WG250 - Netscape Unix (Manual)

From the command line:

cd to the directory where the log files are located

By default the log files are stored where the server configuration files are installed

\netscape\servers\"virtual server name\"logs

The location of the log files can also be found by using the Netscape Administration server.

Locate the Logs tab and look for the Log Files path. Log file names by default are:

Access."date"

Errors."date"

Ex. Access.20040128

File permissions should be set to:

root webadmin 750/640

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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Checks: WG250 - Netscape Windows (Manual)
From the command line:

cd to the directory where the log files are located
By default the log files are stored where the server configuration files are installed

C:\netscape\servers\virtual server name\logs

The location of the log files can also be found by using the Netscape Administration server. Locate the Logs tab and look for the Log Files path. Log file names by default are:

Access."date"
Errors."date"
Ex. Access.20040128

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 - Generic (Manual)

To ensure the integrity of the data that is being captured in the log files, only the members of the Auditors group, Administrators, and the user assigned to run the web server software will be granted permissions to read the log files.

Query the SA to determine who has access to the web server log files.

NOTE: Auditors may have full control of the logs. Also, this does not apply to active log files that require the system account to have full access.

If any account has access to the log files other than those authorized, 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 Systems Standard 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

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 3.9
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WG290 - Netscape Windows (Manual)
Locate the document root via the magnus.conf file. Also, locate any and all scripts directories.

By default, the Netscape anonymous user is anyone. This is not an account on the server, but rather a default construct in the Restrict Access portion of the Administrative Server's menu.

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 or the UNIX 'world' user has access to these directories, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II**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 3.9
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG290 - Netscape Unix (Manual)

In default installs, the user nobody will be the web client account. However, the SA or Web Manager may have created an account such as wwwusr to more explicitly deal with this issue.

Locate the document root via the magnus.conf file. In addition locate and and all scripts or active content directories.

Permissions for these users will be r_x or more restrictive.

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

Vulnerability Key: V0002259**STIG ID:** WG300**Release Number:** 6**Status:** Active**Short Name:** WG300**Long Name:** Web server system files do not conform to minimum file permission requirements.**IA Controls:** ECCD-1 Changes to Data
ECCD-2 Changes to Data**Categories:** 2.2 Least Privilege**Effective Date:** 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: This check verifies that the key web server system configuration files are owned by the SA or Web Manager controlled account. These same files which control the configuration of the web server, and thus its behavior, must also be accessible by the account which runs the web service. If these files are altered by a malicious user, the web server would no longer be under the control of its managers and owners; properties in the web server configuration could be altered to compromise the entire server platform.

Documentable: No**Documentable****Explanation:****Potential****Impacts:****Responsibility:** System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG300 - Netscape Windows (Manual)

The server root is clearly defined in the magnus.conf, obj.conf, and server.xml files, for example:
ServerRoot :/Netscape/Server4/https-admserv

The following permissions can be set on production servers for the given directories.

Create a non-privileged (e.g. NetAdmin) to run the web instance. This account will be part of the server baseline documentation.

cgi-bin/all files
 Administrators (Full Control)
 System (Full Control)
 NetAdmin (Full Control)

config/all files

Administrators (Full Control)
System (Full Control)
NetAdmin (Full Control)

Htdocs/all files
Administrators (Full Control)
System (Full Control)
NetAdmin (Full Control)
Authenticated Users (Read)

Icons/all files
Administrators (Full Control)
System (Full Control)
NetAdmin (Full Control)

Logs /all files
Administrators (Full Control)
System (Full Control)
NetAdmin (Full Control)

If the file permissions are less restrictive that identified above, this is a finding.

NOTE: There may be additional directories based the local implementation, and permissions should apply to directories of similar content. Ex. all web content directories should follow the permissions for htdocs.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

This applies to both SIPRNet and NIPRNet web servers.

If access to a web server by public search engine agents is not restricted, this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category III**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.**Documentable:** No**Documentable
Explanation:
Potential**

Impacts:**Responsibility:** Web Administrator**References:** Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13
8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling**Checks:** WG340 - Netscape (Manual)

From the Administrative Server | select the web site to Manage| Select Preferences tab| Edit Listen Sockets| In the port window make sure port 443 is chosen, if not query SA or Web Manager of the SSL/TLS port. Look for the security window. Make sure ON is set in the pull down menu. Also, select attributes and look to for TLS to be chosen.

*Note: This information can also be found in the magnus.conf file as an entry of:

SSL ON

and the server.xml file as:

Secutritry = ON

port = 443

In the case of a private web server, if encryption is set to OFF, this is a finding.

If there is no entry for an SSL/TLS port, then this is a finding.

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 situation, 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.13

Checks: WG342 - Generic (Manual)

The reviewer should have the SA demonstrate by showing the entry in the web server configuration files that identified the version of SSL that is being used. This can be validated by having the SA show you the properties for the server certificate.

If the web site's server certificate is not utilizing SSL V3.1 / TLS, this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 likely utilizes a content switch to control traffic to the various web servers. In this situation, the SSL certificate 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: V0002227**STIG ID:** WG360**Release Number:** 5**Status:** Active**Short Name:** WG360**Long Name:** Symbolic links are used in the web document (content) directory tree.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 12.4 CM Process**Effective Date:** 01 Dec 1999

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III**Vulnerability Discussion:**

A symbolic link allows a file or directory to be referenced using a symbolic name raising a potential hazard if symbolic linkage is made to a sensitive area. When web scripts are executed and symbolic

links are allowed, the web user could be allowed to access locations on the web server that are outside the scope of the web document root or home directory.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator

Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE

Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG360 - Netscape (Manual)

Locate the directories containing the web content, i.e /usr/local/netscape/server4/docs.

Use ls -al

An entry such as the following would indicate the presence and use of symbolic links:

```
lr-xr--r-- 4000 wwwusr wwwgrp 2345 Apr 15 data -> /usr/local/netscape/server4/docs
```

From the Administrative Server select the web site to manage.

Select the Virtual Server Class | select defaultclass (or created custom class) then Manage | select Content MGMT | Symbolic (Soft) Links will be an option.

The dialog window will offer the option: Allow Soft file links: Select Never for both the server root and document root directories.

Finally, the target file or directory must be owned by the same owner as the link, which should be the non-privileged account with access to the web content.

If any files in the web document directories have symbolic links as evidenced by a l as the first character, and a redirect to another file this is a finding.

Vulnerability Key: V0002228

STIG ID: WG400

Release Number: 3

Status: Active

Short Name: WG400

Long Name: All interactive programs are not placed in a designated directory with appropriate permissions.

IA Controls: DCPA-1 Partitioning the Application

Categories: 2.2 Least Privilege
12.4 CM Process

Effective Date: 01 Dec 1999

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality	I - Mission Critical	II - Mission Support	III - Administrative

Grid:	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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. All CGI program files need to be segregated into their own directory to simplify the protection of these files. Having them in their own directory all to control permissions at the directory level vs. file by file. ASP, JSP, JAVA and PERL scripts are commonly found in these circumstances. Limiting CGI or equivalent scripts to special directories gives the Web Manager or SA control over what goes into those directories. Allowing users to execute CGI scripts in any directory should only be considered if you trust users not to write scripts which will deliberately or accidentally expose the server to an attack. These files, if left in directories from which the anonymous web user could read the source code, would make it easier for someone to understand and attack the web server.

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: WG400 - Unix Netscape (Manual)

Unix does not care what the script is called (no prescribed extension) as long as it has execute permissions. WebUser account read only is adequate

suexec must be enabled. Use httpd -l to check. Results should be: suexec enabled and the path to the cgi-bin directory.

Directory permissions 510 where owner is root, SA or Web Manager and the anonymous web user is represented by the group.

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. 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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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. Apache: suexec must be enabled to ensure that scripts run in the proper context.

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: WG400 - Netscape Windows (Manual)
Windows uses command.com as the default shell and will execute .bat and .exe files. NTFS permissions are: WebUser account (i.e webuser or nobody) – Read and Execute

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. 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 Read/Write permission.

If the CGI script directory has improper access controls this is a finding.

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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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: No

Documentable

Explanation:

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 - Generic (Manual)

Query the SA to determine if and CGI (includes all languages) are used on the server. If CGI programs are being used, check the permissions of these files to ensure they are owned by the non-privileged user running the web server and have proper access controls.

If the CGI programs are not owned by the web server account, this is 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 - Unix (Manual)

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

Using `ls -al`, examine the file permissions on the CGI scripts directory.

If the directory can be accessed by any group that does not require access (i.e. FTP users), 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 Section 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.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 Section 4.5

Checks: WG460 - Unix (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`

1) `grep perl httpd.conf |grep -v '#'`

You should also check /apache/sysconfig.d/loadmodule.conf for perl

NOTE: The name of the loadmodule.conf may vary by installation

If Apache doesn't have the mod_perl module loaded then it doesn't use perl and this is Not Applicable and the check can stop here.

2) grep -i 'PerlTaintCheck' httpd.conf

If 'PerlTaintCheck on' is set, this is not a finding and the check can stop here.

NOTE: If the PerlTaintCheck is a part of an Included config file, this meets the requirement.

3) Check each individual perl script

From the ServerRoot directory: find . -name '*.pl'
From the DocumentRoot directory: find . -name '*.pl'

Examine the beginning of every perl script for -T option. If the -T option is not specified in any perl script, 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

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Site (Target: Netscape Site 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 Section 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 - 33