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: XenApp Web Interface Server

Vulnerability Key: V0018025
STIG ID: CTX0150
Release Number: 2
Status: Active
Short Name: Smart card authentication is set to pass-thru.
Long Name: Smart card authentication is set to pass-thru.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 1.4 Authentication Services
Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: CTX0150
Severity: Category II
Long Name: Smart card authentication is set to pass-thru.

Vulnerability Discussion: When a user selects an application on a Web Interface server, a file is sent to the browser. This file can contain a setting that instructs the client to send the userâ€™s workstation credentials to the server. By default, the client does not honor this setting; however, there is a risk that if the pass-thru feature is enabled on the Presentation Server Client for Win32, an attacker could send the user a file causing the userâ€™s credentials to be sent to an unauthorized or counterfeit server. Secondly, if an attacker was able to access a workstation, and the PIN was cached, they would be able to access XenApp published applications without any authentication prompt. Therefore, smart card authentication will not be set to pass-thru.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0150 (Manual)

On the Web Interface Server, perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Navigate to the Web Interface and right click on the web interface and select "Configure authentication methods".
3. Verify that "Pass-through with smart card" is NOT selected. If it is, this is a finding.
If "Anonymous", "Explicit", or "Pass-Thru", is selected, this is a finding as well.
4. Select the Program Neighborhood Agent website and right click on the config.xml.
5. Select the "Configure authentication methods".
6. Verify that "Pass-through with smart card" is NOT selected. If it is, this is a finding.
If "Anonymous", "Explicit", or "Pass-Thru", is selected, this is a finding as well.

Note: To use smart card authentication, the Web Interface must be running on IIS and users must be running Internet Explorer Version 5.5 or later on 32-bit Windows systems. Secure Sockets Layer (SSL) must be enabled on the Web server. Because SSL is the mechanism underlying smart card technology, SSL must be used between the browser and Web server.

Fixes: SRC-CTX-150 (Manual)

Disable smart-card pass thru authentication.

Vulnerability Key: V0018104

STIG ID: CTX0170

Release Number: 1

Status: Active

Short Name: PNAgent website not using SSL/TLS.

Long Name: Program Neighborhood Agent website is not using SSL/TLS.

IA Controls: ECCT-1 Encryption for Confidentiality (Data in Transit)
ECCT-2 Encryption for Confidentiality (Data in Transit)

Categories: 8.1 Encrypted Data in Transit

Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: CTX0170

Severity: Category II

Long Name: Program Neighborhood Agent website is not using SSL/TLS.

Vulnerability Discussion: Unencrypted XenApp client to server sessions do not protect the information transmitted from being read or viewed by anyone. Unencrypted sessions are vulnerable to a number of attacks to include man-in-the-middle attacks, TCP Hijacking, and replay. Smart card logon and SSL/TLS-secured communications between the client and the server running the Web Interface are not enabled by default. SSL/TLS may be enabled by forcing URLs to apply the HTTPS protocol automatically. The XenApp server must have SSL configured as well for it to work.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0170 (Manual)

To verify that SSL/TLS is configured, perform the following on the XenApp server:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Navigate to Citrix Resources > Configuration Tools > Web Interface > (PNAgent Website Name)
3. Right Click on the config.xml and select Manage Server Settings.
4. Verify that â€œUse SSL/TLS for communications between clients and the Web serverâ€ is checked. If it is, this is a finding.

Fixes:

CTX0170 (Manual)

Use SSL/TLS for all communications between the Program Neighborhood Agent and the Web server.

Vulnerability Key: V0018233

STIG ID: CTX0780

Release Number: 1

Status: Active

Short Name: Web interface servers are not located in DMZ.

Long Name: Web interface servers are not located in the DMZ or screened subnet.

IA Controls: EBRU-1 Remote Access for User Functions

Categories: 4.4 DMZ

Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0780

Severity: Category II

Long Name: Web interface servers are not located in the DMZ or screened subnet.

Vulnerability Discussion: The Web Interface provides user access to published resources in a server farm from a Web browser. The Web Interface works with the Secure Gateway to provide a logon interface, and facilitates authentication and authorization of connection requests to the server farm. The Secure Gateway works with the Web Interface to provide a single, secure, encrypted point of access through the Internet to servers on internal corporate networks. This means remote users can access published applications without compromising network security, from any location at anytime. The Web Interface employs Java and .NET technology executed on a Web server to dynamically create an HTML depiction of server farms for XenApp Server sites that are located within the enclave.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0780 (Manual)

If Web Interface server is located behind the enclave and is only used by internal users, this is Not Applicable.
Check with the Network reviewer or system administrator to obtain the external, internal, and DMZ IP addresses of the firewall. Once these IP addresses have been obtained, review the IP address configuration on Web Interface servers. Access the Web Interface server and type the following at the command prompt:

```
C:\>ipconfig /all
```

1. If the IP address is on the same network as the DMZ firewall interface, this is not a finding.

2. If the IP address listed is on the same internal network as the internal interface of the firewall, this is a finding.

3. If the IP address is on the same network as the outside interface of the firewall, this is a finding.

Fixes: CTX0780 (Manual)

Place the Web Interface server in the DMZ or screened subnet.

Vulnerability Key: V0018234

STIG ID: CTX0790

Release Number: 1

Status: Active

Short Name: Web Interface certs are not approved DoD certs

Long Name: Citrix Web Interface certificates are not DoD approved certificates.

IA Controls: DCNR-1 Non-repudiation

Categories: 1.2 PKI

Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0790

Severity: Category II

Long Name: Citrix Web Interface certificates are not DoD approved certificates.

Vulnerability Discussion: User sessions with the Web Interface server should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from ICA clients. To encrypt session data, the sending component, the client, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, all user sessions with the Web Interface server will be encrypted with a FIPS 140-2 encryption algorithm. The purpose of the PKI certificate is to provide electronic identification of the server, and provide secure encrypted communications between the server and the user. Department of Defense (DoD) servers, identified in DODI 8520.2 as Private Web Servers, require installation of a Public Key Infrastructure (PKI) certificate to support strong authentication and the Secure Sockets Layer (SSL) protocol.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0790 (Manual)

Access the Web Interface server and review the certificates in the following location:
C:\Windows\SSL Relay\keystore\certs
If no valid DoD certificate and private key are present here this is a finding. This directory should contain a DoD certificate and key only (server.crt and server.key). Validate the certificate is listed in the InstallRoot3.12_SAG.pdf document. The DoD certificates that are listed in the InstallRoot3.12_SAG.pdf document are listed in Section 1, Appendix B. If the certificate is not listed here, this is a finding.

Note: The InstallRoot3.12_SAG.pdf document may have been replaced with a newer version. If so, use the most current version listed on the DoD PKE site.

NOTE: The InstallRoot3.12 _SAG.pdf document can be downloaded from the following links:
(Note: These links may have changed since the release of the checklist.)

https://www.us.army.mil/suite/page/474113

OR

https://www.us.army.mil/suite/portal/index.jsp. Select Files and search for the InstallRoot folder. Select the InstallRoot folder and select the InstallRoot3.12_SAG.pdf document to download.

Fixes:

CTX0790 (Manual)

Employ signed DoD certificates on Web Interface server. To create SSL/TLS certificates, the server administrator should use the site certificate ordering processes to obtain DoD PKI certficiates.

Typically, the system administrator must use the Web Server or Web Server operating system tools as appropriate to generate the Public Key Cryptography Standard (PKCS) #10 certificate request. Or the following programs may be used to create and retrieve the signed certificate.
1. Serveral programs are needed to create the openssl certificates. These include Activestate Perl, openssl for Win32, and Visual C++ 2008 Redistribute. To get these programs go to the following websites and download them:

Note: These URL links may have changed since the release of the checklist.

a. Activestate Perl - Use http://www.activestate.com/activeperl/ and click on "ActivePerl Download

Now".

b. Openssl for Win32 â€“ Use http://www.slproweb.com/products.html

c. Visual C++ 2008 Redistribute - Use http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en

2. Navigate to the OpenSSL directory (c:\openssl\bin\) on the Web Interface server.
3. Generate the RSA key for the server and the certificate signing request (CSR):
openssl req -new -out filename.csr
When prompted enter the following: (Do not type the quotations)

For Country Name, type â€œUSâ€
For State or Province Name, type â€œ.â€
For Locality Name, type â€œ.â€
For Organization Name, type â€œU.S. Governmentâ€
For Organizational Unit Name, type â€œOU=DISA, OU=PKI, OU=DoDâ€
For Common Name, type your Fully Qualified Domain Name of your server (i.e.server.disa.mil)
For Email Address, type your email address

4. The output from this command will yield two files: filename.csr and privkey.pem
5. Upload/Copy the filename.csr to the Regular SSL Server Enrollment Form for the DoD PKI site. You may use either of the two sites below.

Note: These Certificate Authorities may have been decommissioned since the release of the checklist. If so, please use the most current Certificate Authority for enrolling your certificate request.

CA-17 URL - https://ca-17.c3pki.chamb.disa.mil/ca
CA-18 URL - https://ca-18.c3pki.den.disa.mil/ca

6. You will be emailed that your certificate is ready and you will retrieve your signed certificate from the CA.
7. In addition, you must create a PFX-formatted certificate file specific for Windows. The filename.pfx file is a concatenation of the serverâ€™s certificate and private key, exported in the PFX format; this file is then copied to the sub-directory on the XenApp server.
Perform the following command: (filename is the name of your certificate file)
C:\openssl\bin\Openssl pkcs12 â€“export in filename.crt â€“inkey privkey.pem â€“name filename â€“passout pass:testpassword â€“out filename.pfx
8. Put the new signed certificate, private key, and filename.pfx in the C:\Windows\System32\certsrv\CertEnroll\ directory or the appropriate certificate directory. Move any old certificates from the directory and put them somewhere safe for backup purposes.

Vulnerability Key:	V0018235
STIG ID:	CTX0800
Release Number:	1
Status:	Active
Short Name:	Web Interface Server to ICA clients is not HTTPS
Long Name:	The Web Interface Server to ICA client traffic is not configured for HTTPS.
IA Controls:	ECCT-1 Encryption for Confidentiality (Data in Transit) ECCT-2 Encryption for Confidentiality (Data in Transit)
Categories:	8.1 Encrypted Data in Transit
Effective Date:	29 Jun 2009

□ Open □ Not a Finding	Comments:

□ Not Applicable □ Not Reviewed	

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0800

Severity: Category II

Long Name: The Web Interface Server to ICA client traffic is not configured for HTTPS.

Vulnerability Discussion: Attackers can exploit Web Interface data as it crosses the network between the Web server and browser and as it is written on the client device itself. An attacker can intercept logon data, the session cookie, and HTML pages in transit between the Web server and Web browser. Although the session cookie used by the Web Interface is transient and disappears when the user closes the Web browser, an attacker with access to the client deviceâ€™s Web browser can retrieve the cookie and possibly use credential information. Although the ICA file does not contain any user credentials, it contains a one-time use ticket that expires in 200 seconds, by default. An attacker may be able to use the intercepted ICA file to connect to the server before the authorized user can use the ticket and make the connection. If single sign-on is enabled, an attacker could send the user an ICA file that causes the userâ€™s credentials to be misrouted to an unauthorized or counterfeit server. Therefore, all client traffic to the Web Interface server will be encrypted.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0800 (Manual)

If the Secure Gateway is installed on the same server as the Web Interface and clients are connecting to the Secure Gateway first, proceed to step 6.
1. Select Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager.
2. In the Console tree, right click on the Default Web Site, and click properties.
3. Select the Directory Security tab and click Edit.
4. Verify that â€œRequire secure channel (SSL)â€ and â€œRequire 128 bit encryptionâ€ are both checked. If not, this is a finding.
5. Select the Web Site tab and verify that â€œSSL Port: 443â€ is configured. If not, this is a finding.
6. Launch the Web Interface Console (via the Access Management Console). Right-click the Web Interface Site > Manage secure client access > Edit Gateway settings.
7. Verify that the Secure Gateway is listed in the Address (FQDN): section with port 443. If these are not listed, this is a finding.

Fixes: CTX0800 (Manual)

Configure the Web Interface server to use SSL for all communications with clients.

Vulnerability Key: V0018237

STIG ID: CTX0810

Release Number: 1

Status: Active

Short Name: Web Interface traffic to the STA is unencrypted.

Long Name: Web Interface server traffic to the Secure Ticket Authority (STA) is unencrypted.

IA Controls: ECCT-1 Encryption for Confidentiality (Data in Transit)
ECCT-2 Encryption for Confidentiality (Data in Transit)

Categories: 8.1 Encrypted Data in Transit

Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0810

Severity: Category II

Long Name: Web Interface server traffic to the Secure Ticket Authority (STA) is unencrypted.

Vulnerability Discussion: The Web Interface traffic uses the XML protocol to exchange data with the XenApp server. XML traffic contains usernames, scrambled passwords, and application lists. The XML protocol uses plaintext to exchange all data except for passwords. An attacker may intercept the XML protocol traffic and steal application set information, user passwords, and potentially crack the obfuscation. An attacker may also impersonate the server and intercept authentication requests. Therefore, XML traffic between the XenApp server and the Web Interface will be encrypted. An alternative to encrypting the traffic is to run the Web Interface on the XenApp server within the enclave.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0810 (Manual)

Access the Web Interface server and perform the following:
1. Open Windows Explorer and navigate to the following:
C:\Inetpub\wwwroot\Citrix\AccessPlatform\conf.
2. Open the WebInterface.conf file.
3. Verify the Farm1= {The FQDN of the XenApp server in the enclave}, if it does not have the correct name of the farm, this is a finding. Note: The server name must match the name on the XenApp serverâ€™s DoD certificate.
4. Verify the value of the Transport and SSLRelayPort settings in the XenApp farm parameter is configured to the following: XML Port: 80, Transport: HTTPS, SSLRelayPort: 443. If they are not, this is a finding.

Fixes:

CTX0810 (Manual)

Encrypt all XML traffic from the Web Interface server to the XenApp server.

Vulnerability Key: V0018239

STIG ID: CTX0820

Release Number: 2

Status: Active

Short Name: The Web Interface is not configured for smart card

Long Name: The Web Interface is not configured for smart card authentication.

IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication

Categories: 1.4 Authentication Services

Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0820

Severity: Category II

Long Name: The Web Interface is not configured for smart card authentication.

Vulnerability Discussion: Two-factor authentication identifies users using two distinctive factors--something they have and something they know or something they are. Requiring two different forms of electronic identification reduces the risk of fraud. Something a user has can be a physical device sometimes referred to as a token. Token options include smart-tokens, smart cards, and password generation tokens. Smart cards may be enabled within the Citrix XenApp Server environment. Smart cards are small plastic cards with embedded computer chips. Within the DoD environment, this would be the Common Access Card (CAC) or Alternate Smart Card Login (ALSC) which is used for privileged account access to networks. Smart cards authenticate users to networks and computers, secure channel communications over a network, and use digital signatures for signing content. With smart cards, a userâ€™s private key is securely stored within the smart card and never leaves the card. Using the onboard processor, all cryptographic functions, including digital signatures and decryption of session keys, occur inside the card. Smart cards will be used for authentication when users access applications and content published on servers. In addition, Citrix supports two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is employed to prove that the cardholder is the rightful owner of the smart card.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0820 (Manual)

To verify smart card is enabled for the Web Interface server, perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Select Citrix Resources > Configuration Tools > Web Interface > (Web Interface site)
3. Right Click on the site and select Configure authentication methods.
4. Verify smart card is checked. If it is not, this is a finding.

Note: To use smart card authentication, the Web Interface must be running on IIS and users must be running Internet Explorer Version 5.5 or later on 32-bit Windows systems. Secure Sockets Layer (SSL) must be enabled on the Web server. Because SSL is the mechanism underlying smart card technology, SSL must be used between the browser and Web server.

Fixes: CTX0820 (Manual)

Enable smart card authentication for the Web Interface server.

Vulnerability Key: V0018240
STIG ID: CTX0830
Release Number: 1
Status: Active
Short Name: Inactive Web Interface sessions don't have timeout
Long Name: Inactive Web Interface sessions are not configured with a timeout value.
IA Controls: EBRP-1 Remote Access for Privileged Functions
Categories: 1.4 Authentication Services
Effective Date: 29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0830

Severity: Category II

Long Name: Inactive Web Interface sessions are not configured with a timeout value.

Vulnerability Discussion: The default inactive Web Interface session timeout is 20 minutes. The Web Interface server should restrict inactive sessions to 10 minutes or less to comply with other STIG guidance. Leaving sessions open longer than 10 minutes ensures limits exist and are configured on how long published applications will remain available on the server. If the session time is kept open indiscriminately, users may get distracted and walk away from the client device leaving the session accessible to unauthorized users.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0830 (Manual)

To verify "Session Timeout" is configured for the Web Interface server, perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Select Citrix Resources > Configuration Tools > Web Interface > (Web Interface site)
3. Right Click on the site and select Manage Session Preferences.
4. Verify that â€œSession Timeoutâ€ is configured to 10 Minutes or less. If not, this is a finding.

Fixes:

CTX0830 (Manual)

Configure inactive session limits for Web Interface server.

Vulnerability Key:	V0018242
STIG ID:	CTX0840
Release Number:	2
Status:	Active
Short Name:	The Web Interface Server is not configured in VMS
Long Name:	The Web Interface Server is not configured in VMS with the correct posture
IA Controls:	VIVM-1 Vulnerability Management
Categories:	12.5 IAVM Process
Effective Date:	29 Jun 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0840

Severity: Category II

Long Name: The Web Interface Server is not configured in VMS with the correct posture

Vulnerability Discussion: Correctly configuring XenApp assets in VMS will ensure that the appropriate vulnerabilities are assigned to the asset. If the asset is not configured with the correct posture, vulnerabilities may be open on the asset. These open vulnerabilities may allow an attacker to access the system.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0840 (Manual)

1. If VMS is not used, this check is Not Applicable.
2. If the assets are registered, verify that the following postures are registered. If any of the postures are not registered, this is a finding.

Win2k3
AntiVirus
IIS 6.0
XenApp Web Interface Server

Fixes: CTX0840 (Manual)

Configure all Web Interface assets into VMS with the correct posture.

Vulnerability Key:	V0021549
STIG ID:	CTX0835
Release Number:	1
Status:	Active

Short Name: The WebInterface Server is not registered in VMS.

Long Name: The WebInterface Server is not registered in VMS or vulnerability database.

IA Controls: VIVM-1 Vulnerability Management

Categories: 12.5 IAVM Process

Effective Date: 14 Oct 2009

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

Condition: XenApp Web Interface Server (Target: XenApp Web Interface Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0835

Severity: Category II

Long Name: The WebInterface Server is not registered in VMS or vulnerability database.

Vulnerability Discussion: The Vulnerability Management System (VMS) was developed to interface with the DoD Enterprise tools to assist all DoD CC/S/As in the identification of security vulnerabilities and track the issues through the lifecycle of the vulnerabilities existence. To ensure both the emerging and known vulnerabilities are addressed on a system, VMS tracks the existence of all potential vulnerabilities based on the posture of an asset. Therefore, all vulnerabilities are tracked through their lifecycle. Vulnerability Management is the process of ensuring that all network assets that are affected by an IAVM notice are addressed and corrected within a time period specified in the IAVM notice. VMS will notify commands, services, and agencies of new and potential security vulnerabilities. VMS meets the DoD mandate to ensure information system vulnerability alert notifications are received and acted on by all SAs. Keeping the inventory of assets current allows for tracking of XenApp servers and resources, and supports a successful IAVM process. The ability to track assets improves the effective use of WebInterface assets, information assurance auditing efforts, as well as optimizing incident response times.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0835 (Manual)

If VMS is used, then ensure the WebInterface servers are registered within VMS. If they are not registered, this is a finding.
If the site is using another vulnerability database system, then have the IAO demonstrate compliance. If assets are not registered, this is a finding.

Fixes: CTX0835 (Manual)

Register WebInterface servers in VMS or vulnerability management database.

Vulnerability Count - 10