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 Server

Vulnerability Key: V0018016
STIG ID: CTX0090
Release Number: 2
Status: Active
Short Name: Client drive mappings are enabled.
Long Name: Client drive mappings are enabled on the XenApp Server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0090
Severity: Category I
Long Name: Client drive mappings are enabled on the XenApp Server.

Vulnerability Discussion: Client drive mappings are local client drives that are mapped to the XenApp Server and displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive. Client drive mappings pose a security risk because they allow the client to read and write from their local drives and copy or move files to the XenApp server. This allows users to transfer any type of file onto the server that may be malware or malicious code. Transferring files from client devices to the XenApp server could fill up available disk space and create a denial of service to the users, or infect the server with a virus that could affect the availability and integrity of the XenApp server.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0090 (Manual)

Access the XenApp Server and perform the following:
1. Select Start > Administrative Tools > Terminal Services Configuration > ICA-tcp
2. Select the Client Settings tab and verify that under the "Disable the following: Drive Mapping" is checked. If it is not checked, this is a finding.

Fixes: CTX0090 (Manual)

Disable Client drive mappings on all XenApp Servers.

Vulnerability Key: V0018017
STIG ID: CTX0100
Release Number: 2
Status: Active
Short Name: Clipboard mapping is enabled on XenApp Server.
Long Name: Clipboard mapping is enabled on the XenApp Server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0100
Severity: Category II
Long Name: Clipboard mapping is enabled on the XenApp Server.
Vulnerability Discussion: Users may run local and the remote ICA applications (published applications) at the same time. Even though both sets of applications are running on different computers, the clipboard option is available with the ICA software. If Clipboard Mapping is enabled for ICA connections, users may cut and paste between the local application and the remote ICA application. Clipboard mapping allows

any data that is written to the clipboard of either the client or the server is instantly replicated to the clipboard of the other. The clipboard mapping allows any type of data to be written to the client drive or server drive. If the XenApp server has malicious code on the server, a client workstation could be infected with this malicious code. Text objects may be transferred, such as passwords, which could compromise the XenApp server. This may cause information leakage and potentially infect other operating systems if the text is a string that can be run as a command or URL. Therefore, clipboard mapping will be disabled to prevent file transfers that may be malicious to the client or server via the clipboard.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0100 (Manual)

Access the XenApp server and perform the following:
1. Select Start > Administrative Tools > Terminal Services Configuration > ICA-tcp
2. Select the Client Settings tab.
3. Verify that under "Disable the following: Clipboard Mapping" is checked. If it is not checked, this is a finding.

Fixes: CTX0100 (Manual)

Disable Clipboard mapping on all XenApp Servers.

Vulnerability Key: V0018106
STIG ID: CTX0190
Release Number: 1
Status: Active
Short Name: ICA traffic is not encrypted.
Long Name: XenApp Independent Computing Architecture (ICA) client traffic is not encrypted with 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 Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0190
Severity: Category II
Long Name: XenApp Independent Computing Architecture (ICA) client traffic is not encrypted with SSL/TLS.
Vulnerability Discussion: XenApp ICA client traffic may be intercepted by an attacker. ICA sessions do not protect the information transmitted from being read or viewed by anyone. Sessions are vulnerable to a number

of attacks to include man-in-the-middle attacks, TCP Hijacking, and replay. Information that may be obtained may include user credentials and client session information including text.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0190 (Manual)

Access the XenApp server and perform the following:
1. Select Start > All Programs > Citrix > Administration Tools > Citrix SSL Relay Configuration Tool
2. On the Relay Credentials Tab, verify that the "Enable SSL relay"□ box is checked and a valid DoD server certificate is selected. If it is not, this is a finding.
3. On the Connection Tab, verify the Encryption Standard selected is "TLSv1"□. If it is not, this is a finding.
4. Verify the Server Name is a fully qualified domain name of the XenApp server and the ports listed include 1494 (ICA traffic is Port 1494). If this is not listed, this is a finding.
5. Select the Ciphersuites Tab, and verify the GOV ciphersuites is selected. If it is not, this is a finding. Verify COM is not selected, if so, this is a finding.
The COM ciphersuites are: SSL_RSA_WITH_RC4_128_MD5 and SSL_RSA_WITH_RC4_128_SHA
The GOV ciphersuite is: SSL_RSA_WITH_3DES_EDE_CBC_SHA
6. Open the Access Management Console, select a published application in the left pane by selecting Citrix Access Management Console > Citrix Resources > Presentation Server > your farm name > Applications > <application name>.
7. From the Action menu, select Modify application properties > Modify all properties.
8. In the Application Properties dialog box, select Advanced > Client options.
9. In the Connection encryption section, verify the following are configured:
"□ Verify the Enable SSL and TLS protocols check box is checked. If not, this is a finding. This option requests the use of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols for clients connecting to the published application.
"□ In the Encryption section, ensure the FIPS -140 (128-bit RC5) encryption is selected. If not, this is a finding.
"□ Verify the Minimum requirement check box is checked. If not, this is a finding. This is only available if you increase the level of ICA protocol encryption. The Minimum requirement check box sets a requirement that Program Neighborhood clients connecting to a published application use the specified level of encryption or higher. This means Program Neighborhood"□s connections to the server are encrypted at the level on the server. If it is not checked, the encryption level used is from the Program Neighborhood client.

Fixes: CTX0190 (Manual)

Encrypt all ICA traffic through the use of SSL/TLS.

Vulnerability Key: V0018107
STIG ID: CTX0200
Release Number: 1
Status: Active
Short Name: XenApp Server is hosting other applications.
Long Name: XenApp server is hosting other applications.
IA Controls: DCPA-1 Partitioning the Application
Categories: 14.4 Unneeded Ports, Protocols, Hardware, and Services
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0200

Severity: Category II

Long Name: XenApp server is hosting other applications.

Vulnerability Discussion: XenApp availability is critical since it controls and manages the entire application publishing infrastructure. XenApp should be installed on a dedicated physical server or virtual machine, since running multiple applications on a XenApp server poses an availability risk. Applications installed on the XenApp server that are not used as published applications should be removed. This is not applicable to operating system programs required for the OS to function. Hosting other applications on XenApp Servers may have many active processes, and privileged users defined. These applications may provide a simple means by which a privileged user unintentionally introduces malicious code onto the server. Therefore, XenApp servers will only run those necessary applications that are required.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0200 (Manual)

Access the XenApp server and perform the following:
1. Select Start > All Programs > Citrix
2. All XenApp components should be listed under Citrix. The Citrix XenApp components may include the following:

Citrix Licensing
Access Management Console
Web Interface
Citrix Presentation Server
Presentation Server Console
Documentation Center

3. Select Start> All Programs
4. Review all the programs listed to ensure that only published applications and OS programs are installed. If third party applications are installed on server, then ask the IAO/SA what they are for. If they are unrelated to the XenApp application, this is a finding.
5. Select Start > Control Panel > Administrative Tools > Services
Review all the running services to verify only those services required by Citrix XenApp are running. If DHCP, DNS, WINS, Remote Access/VPN server, Mail, or other services are running that are not required, this is a finding. (This does not apply to client services)

Fixes: CTX0200 (Manual)

Configure all XenApp servers with only the necessary published applications and OS programs. Remove all third party applications and services that do not support the XenApp application.

Vulnerability Key: V0018109
STIG ID: CTX0210
Release Number: 2
Status: Active

Short Name: XenApp Server not using DoD approved certs.
Long Name: Citrix XenApp 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 Server (Target: XenApp Server)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: CTX0210
Severity: Category II
Long Name: Citrix XenApp certificates are not DoD approved certificates.
Vulnerability Discussion: User sessions with the XenApp 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 XenApp 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: CTX0210 (Manual)

Employ signed DoD approved and current certificates on XenApp servers.
1. Access the XenApp 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:

CTX0210 (Manual)

Employ signed DoD certificates on Citrix XenApp 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 - 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 XenApp 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 "US"
For State or Province Name, type "."
For Locality Name, type "."
For Organization Name, type "U.S. Government"
For Organizational Unit Name, type "OU=DISA, OU=PKI, OU=DoD"
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 server"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 -export in filename.crt -inkey privkey.pem -name filename -passout pass:testpassword -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: V0018110
STIG ID: CTX0220
Release Number: 2
Status: Active
Short Name: The STA does not use TLS
Long Name: The Secure Ticket Authority (STA) is not configured to use 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 Server (Target: XenApp Server)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: CTX0220
Severity: Category II
Long Name: The Secure Ticket Authority (STA) is not configured to use TLS.
Vulnerability Discussion: The STA role is to issue session tickets in response to connection requests from the Secure Gateway or Web Interface Servers. The STA also uses the tickets as a foundation for authentication and authorization for access to published applications in the farm. When the client connects to the Secure Gateway Server, the ticket is presented and the Secure Gateway Server must validate the ticket before establishing a secure session for the client. The Secure Gateway Server performs a data request by sending the ticket back to the STA and asking for its corresponding data in return. If successfully validated, the Secure Gateway Server establishes a relay between the end user and the XenApp Server. The traffic between the STA and the Secure Gateway or Web Interface servers are HTTP based. Encrypting this traffic will ensure that an attacker cannot intercept the ticket as it travels from the server to the client. Encrypting the STA traffic will provide confidentiality for session tickets as well as the authentication and authorization information as it travels from server to server.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0220 (Manual)

To configure the STA to utilize SSL, perform the following:
1. Access the XenApp server that is acting as the STA server.
2. Edit the CtxSta.config file located at C:/Program Files\Citrix\System32
3. Search for the "□SSLOnly=off"□. This should be set to "□SSLOnly=on"□. If it is not configured to "□on"□, this is a finding.
4. Select Start > All Programs > Citrix > Administration Tools > Citrix SSL Relay Configuration Tool
5. On the Relay Credentials Tab, verify that the "Enable SSL relay"□ box is checked and a valid DoD server certificate is selected. If it is not, this is a finding.
6. On the Connection Tab, verify that the Encryption Standard selected is "TLSv1"□. If it is not, this is a finding.
7. Verify that the Server Name is a fully qualified domain name of the XenApp server and the port listed is 80, which is the default. The XML port may be configured to another port number, and if it

is, this must be documented with the IAO. If the XML port is not documented with the IAO or port 80 is not listed, this is a finding.
8. Select the Ciphersuites Tab, and verify that the GOV ciphersuites is selected. If it is not, this is a finding. Verify COM is not selected, if so, this is a finding.
The COM ciphersuites are: SSL_RSA_WITH_RC4_128_MD5 and SSL_RSA_WITH_RC4_128_SHA
The GOV ciphersuite is: SSL_RSA_WITH_3DES_EDE_CBC_SHA

Fixes: CTX0220 (Manual)
Configure the STA to use SSL.

Vulnerability Key: V0018126
STIG ID: CTX0230
Release Number: 3
Status: Active
Short Name: STA does not have correct TicketTimeout value.
Long Name: The Secure Ticket Authority (STA) is not configured with a correct TicketTimeout value.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0230
Severity: Category II
Long Name: The Secure Ticket Authority (STA) is not configured with a correct TicketTimeout value.
Vulnerability Discussion: The STA role is to issue session tickets in response to connection requests from the Secure Gateway or Web Interface Servers. The STA also uses the tickets as a foundation for authentication and authorization for access to published applications in the farm. When the client connects to the Secure Gateway Server, the ticket is presented and the Secure Gateway Server must validate the ticket before establishing a secure session for the client. The Secure Gateway Server performs a data request by sending the ticket back to the STA and asking for its corresponding data in return. If successfully validated, the Secure Gateway Server establishes a relay between the end user and the XenApp Server. The STA TicketTimeout value should be no greater than 100000 milliseconds or 100 seconds. Reducing the TicketTimeout value will decrease the amount of time an attacker may transfer the ticket from one machine to another.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

CTX0230 (Manual)

To verify the STA server is configured with the correct TicketTimeout value, perform the following:
1. Access the XenApp server that is acting as the STA server.
2. Edit the CtxSta.config file located at C:\Program Files\Citrix\System32. If the file is not in this location, then do a search for the file on the system by going to Start > Search > For Files and Folders. Type in CtxSta.config.
3. Search for the "□TicketTimeout=100000"□. This should be set to "□TicketTimeout=100000"□. If it is not configured to 100000 or less, this is a finding.

Fixes: CTX0230 (Manual)

Configure the TicketTimeout value to 10000 or less.

Vulnerability Key: V0018128
STIG ID: CTX0240
Release Number: 2
Status: Active
Short Name: The STA does not keep logs for 30 days.
Long Name: The Secure Ticket Authority (STA) is not configured to maintain 30 days of logs online and 1 year offline.
IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting
Categories: 10.4 Reporting
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0240
Severity: Category III
Long Name: The Secure Ticket Authority (STA) is not configured to maintain 30 days of logs online and 1 year offline.
Vulnerability Discussion: The STA role is to issue session tickets in response to connection requests from the Secure Gateway or Web Interface Servers. The STA also uses the tickets as a foundation for authentication and authorization for access to published applications in the farm. When the client connects to the Secure Gateway Server, the ticket is presented and the Secure Gateway Server must validate the ticket before establishing a secure session for the client. The Secure Gateway Server performs a data request by sending the ticket back to the STA and asking for its corresponding data in return. If successfully validated, the Secure Gateway Server establishes a relay between the end user and the XenApp Server. Storing log files for at least 30 days will provide enough time to review activities of users. Log files enable the enforcement of individual accountability by creating a reconstruction of events. They also assist in problem identification that

may lead to problem resolution. If the STA log files are not retained, there is no way to trace or reconstruct the events, and if it was discovered the network was hacked, there would be no way to trace the full extent of the compromise.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0240 (Manual)

Interview the IAO to determine the retention and storage of the STA Server logs.

To check whether the STA is configured to maintain 30 days of logs, perform the following:
1. Access the XenApp server that is acting as the STA server.
2. Open the CtxSta.config file with Notepad located at C:\Program Files\Citrix\System32. If the file is not in this location, then do a search for the file on the system by going to Start > Search > For Files and Folders. Type in CtxSta.config.
3. Search for the "□MaxLogCount=30"□. This should be set to "□MaxLogCount=30"□. If it is not configured to 30, this is a finding.
4. Verify the "LogLevel=0" is set to "Loglevel=3". If not, this is a finding.
4. Ask the IAO if the STA logs are archived for one year. If they are not being archived, this is a finding. If they are archived, request to see the location of the logs for verification.

Fixes: CTX0240 (Manual)

Configure the STA service to log for 30 days.

Vulnerability Key: V0019183
STIG ID: CTX0250
Release Number: 2
Status: Active
Short Name: The STA logs are not restricted.
Long Name: The XenApp Server acting as the STA Server is not configured to restrict the STA logs to authorized users.
IA Controls: ECTP-1 Audit Trail Protection
Categories: 2.1 Object Permissions
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0250

Severity: Category II

The XenApp Server acting as the STA Server is not configured to restrict the STA logs to

Long Name: authorized users.

Vulnerability Discussion: Logs form a recorded history or audit trail of the STA server events, making it easier for system administrators to track down intermittent problems, review past events, and piece together information if an investigation is required. Without this recorded history, potential attacks and suspicious activity will go unnoticed. It is critical to protect STA log files from being modified or accessed by unauthorized individuals. Some logs may contain sensitive data that should only be available to authorized users.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation

Checks: CTX0250 (Manual)

Verify the STA logs are restricted to only authorized users by performing the following:
1. Navigate on the server acting as the STA server %systemroot% \Program Files\Citrix\System 32 \CtxSTA.config. If the file is not in this location, then do a search for the file on the system by going to Start > Search > For Files and Folders. Type in CtxSta.config.
2. Open the CtxSTA.config file with notepad and verify that the location of the Log Directory is set to "LogDir=%systemroot%\Program Files\Citrix\logs\ If this is set to another location, then use that location in step 3.
3. Navigate to %systemroot&\Program Files\Citrix\logs folder.
4. Right click on the "logs" folder and select the Security tab.
5. Ensure that the only groups configured with access greater than READ are configured:
Auditors (Could be Active Directory Group or Local Machine Group)
System
Network Service

If other groups or users are listed with greater than READ access, this is a finding.

Fixes: CTX0250 (Manual)

Restrict access to the STA logs to only authorized users.

Vulnerability Key: V0018135
STIG ID: CTX0260
Release Number: 1
Status: Active
Short Name: Unauthorized users have access to Mgmt. Consoles.
Long Name: Unauthorized users have access to the Access Management and Presentation Server Consoles.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.1 Object Permissions
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: CTX0260

Severity: Category II

Long Name: Unauthorized users have access to the Access Management and Presentation Server Consoles.

Vulnerability Discussion: The Access Management and Presentation Server Consoles are the main user interfaces for managing the XenApp farm. The Access Management Console provides the ability to manage applications, servers, hotfixes, trace logs, performance, client sessions, and administrators. The Presentation Server Console provides the ability to manage zones, policies, printers, isolation environments, and the resource manager. Access to these consoles will be restricted based on authorization by the IAO/SA. Without restrictions to these consoles, a malicious user may reconfigure the XenApp farm and deny XenApp resources to users or open up known vulnerabilities (shadowing, client drive mappings, etc.)

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0260 (Manual)

Access the XenApp server and perform the following:
1.Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Select the <farm name> Administrators.
3. Review the users listed and compare this to the documentation provided by the IAO/SA. If a discrepancy exists, this is a finding.

Fixes: CTX0260 (Manual)

Configure and document all authorized users that need access to the XenApp management consoles.

Vulnerability Key: V0018152

STIG ID: CTX0290

Release Number: 1

Status: Active

Short Name: Concurrent connections are not limited.

Long Name: Users do not have a maximum number of concurrent connections configured.

IA Controls: ECLO-1 Logon
ECLO-2 Logon

Categories: 12.4 CM Process

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: CTX0290

Severity: Category II

Long Name: Users do not have a maximum number of concurrent connections configured.

Vulnerability Discussion: A limit on connections applies to each user who connects to the XenApp server farm. A user"□s active sessions and disconnected sessions are counted for the user"□s total number of concurrent connections. For instance, if a limit of three concurrent connections is configured, and the user tries to establish a fourth, the limit prevents the additional connection. A message tells the user that a new connection is not allowed. Restricting users to a connection limit will ensure that denial-of-service attacks don"□t occur by a malicious user running multiple connections to the server farm and consume server resources and connection license counts. Connection control affects users only if a connection attempt is prevented. If a user"□s number of connections exceeds a connection limit, the client displays a message that describes why the connection is not available. Note: Depending on the XenApp Server hardware specifications, the maximum number of concurrent connections may differ significantly from server to server. Therefore, no specific maximum number of concurrent connections are specified in the check procedure.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0290 (Manual)

Access the XenApp server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Select the farm in the scope pane of the Access Management Console and
select Action > Modify farm properties > Modify all properties.
3. Open the Connection Limits page in the farm"□s Properties list.
4. Verify the "Maximum connections per user"□ is configured with a number to limit each user"□s concurrent connections. If no number is configured, this is a finding.

Fixes: CTX0290 (Manual)

Configure a concurrent connection limit for all users

Vulnerability Key: V0018153

STIG ID: CTX0300

Release Number: 1

Status: Active

Short Name: Shadowing is enabled for XenApp farm.

Long Name: Shadowing is enabled for the XenApp farm.

IA Controls: EBRP-1 Remote Access for Privileged Functions
ECSC-1 Security Configuration Compliance

Categories: 2.2 Least Privilege

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0300

Severity: Category I

Long Name: Shadowing is enabled for the XenApp farm.

Vulnerability Discussion: Shadowing is used to monitor and interact with user sessions. User shadowing allows the administrator to view everything that appears on the user"□s session display. Administrators may also use the keyboard and mouse remotely while shadowing the user"□s session. Because of the unobstructed access to a user's session, shadowing creates a security issue. An attacker or malicious administrator who has administrative privileges on the XenApp Server could use the shadowing feature of XenApp to observe the actions of other users without detection. Furthermore, a user policy may be created to enable user-to-user shadowing. User-to-user shadowing allows users to shadow other users without requiring them to be members of the Citrix administrator group. User-to-user shadowing allows multiple users from different locations to view user sessions, allowing one-to-many, many-to-one, and many-to-many scenarios. These situations could easily result in the disclosure of confidential information or modification of user session data. Therefore, shadowing will be disabled.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0300 (Manual)

Access the XenApp server and perform the following:
1. Start > Run > and type "regedit"□, enter
2. Verify the following key is configured to 0: HKLM\SYSTEM\Current Control Set\Control\Terminal Server\WinStations\ICA-tcp\Shadow
3. Value must be set to 0. If not, this is a finding.

Fixes: CTX0300 (Manual)

Disable shadowing for the XenApp server farm.

Vulnerability Key: V0018154

STIG ID: CTX0310

Release Number: 2

Status: Active

Short Name: Shadow executable permissions are not restrictive.

Long Name: Shadow executable permissions are not restrictive.

IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data

Categories: 2.1 Object Permissions

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0310

Severity: Category II

Long Name: Shadow executable permissions are not restrictive.

Vulnerability Discussion: An attacker or malicious administrator who has administrative privileges on the XenApp server could use the shadowing feature of XenApp to observe actions of other users. Such a situation could result in the disclosure of confidential information. Even if shadowing is disabled for the farm, users may still be able to execute the shadow executable and view user sessions. The Cshadow.exe is a command line executable that acts as the shadowing engine for all XenApp shadow utilities. It"□s located in C:\Program Files\Citrix\System32 and is invoked anytime a shadow session is launched. As an added security measure, the permissions on this executable should be restricted.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0310 (Manual)

Access the XenApp server and perform the following:
1. Select Windows explorer and navigate to C:\Program Files\Citrix\System32. If the Cshadow.exe is not in this location, then do a search for the file on the system by going to Start > Search > For Files and Folders. Type in Cshadow.exe.
2. Right click on the Cshadow.exe, select the security tab and ensure that only the following users are listed:

Administrators
SYSTEM

If there are other users listed, this is a finding.
3. Request documentation from the IAO for all users listed in the Administrators group. If users are listed that are not documented with the IAO, then this is a finding.

Fixes: CTX0310 (Manual)

Restrict access to the shadow executable.

Vulnerability Key: V0018155

STIG ID: CTX0320

Release Number: 1

Status: Active

Short Name: Re-authentication is not required for reconnection

Long Name: Clients are not prompted for authentication upon an ICA session reconnection.

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	Comments:

☐ Not Applicable ☐ Not Reviewed	

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0320

Severity: Category II

Long Name: Clients are not prompted for authentication upon an ICA session reconnection.

Vulnerability Discussion: The Auto Client Reconnect feature allows Clients for Windows, Java, and Windows CE to detect broken connections and automatically reconnect users to disconnected sessions. When a client detects an involuntary disconnection of a session, it attempts to reconnect the user to the session until there is a successful reconnection or the user cancels the reconnection attempts. When a connection breaks, it may leave the server session in an active state. Users can reconnect only to sessions that are in a disconnected or inactive state. Cookies containing keys to user credentials and session IDs are created on the client device when sessions are started. Because users can be reconnected only to disconnected sessions, Auto Client Reconnect uses the cookie on the client device to disconnect an active session before attempting to reconnect. By default, Auto Client Reconnect is enabled at the server farm level, and user re-authentication is not required. The Auto Client Reconnect will be configured to require user authentication. This will ensure that users are prompted to re-authenticate for all interrupted sessions.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0320 (Manual)

Access the XenApp server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Select the farm in the scope pane of the Access Management Console and
select Action > Modify farm properties > Modify all properties.
3. Open the Auto Client Reconnect page in the farm"□s Properties list.
4. Verify the "Require user authentication"□ is selected. If not, this is a finding. If the "Reconnect automatically"□ is selected, this is a finding.

Fixes: CTX0320 (Manual)

Configure re-authentication for all broken ICA connections.

Vulnerability Key: V0018156

STIG ID: CTX0330

Release Number: 1

Status: Active

Short Name: Disconnected sessions have no time limit.

Long Name: XenApp server is not configured with a time limit for disconnected sessions.

IA Controls: EBRP-1 Remote Access for Privileged Functions

Categories: 12.4 CM Process

Effective Date: 29 Jun 2009

	Comments:

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0330

Severity: Category II

Long Name: XenApp server is not configured with a time limit for disconnected sessions.

Vulnerability Discussion: Session Reliability is available with the Enterprise and Advanced Editions of Citrix Presentation Server. This feature keeps sessions active and on the user"□s screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes. With Session Reliability, the "Seconds to keep sessions active"□ option has a default of 180 seconds, or three minutes. If there is no time limit a session is kept open indiscriminately, then chances increase that a user may get distracted and walk away from the client device, potentially leaving the session accessible to unauthorized users. The "Seconds to keep sessions active" time will be set to 60 seconds or less.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0330 (Manual)

Session Reliability is only available with the Enterprise and Advanced Editions of Citrix Presentation Server. If the XenApp Server is not running one of these edtions, this check is Not Applicable.

To check the version, access the Access Management Console:
1. Select a farm in the scope pane of the Access Management Console and Navigate to the XenApp farm > Servers
2. Select the appropriate server and right click on it. Select Information from the drop down menu.
3. The Information section will have the Product and Version information displayed. If the Enterprise or Advanced Editions are listed, proceed to step 4. Otherwise this is Not Applicable.
4. Select Start > All Programs > Citrix > Management Consoles > Access Management Console
5. Select the farm in the scope pane of the Access Management Console and select Action > Modify farm properties > Modify all properties.
6. Open the Session Reliability page in the farm"□s Properties list.
7. Verify the "Allows users to view sessions during broken connection"□ is selected. If this is not selected, this is a finding. Ensure the "Seconds to keep sessions active"□ is configured to 60 seconds or less. Anything greater than 60 seconds is a finding.

Fixes: CTX0330 (Manual)

Configure a time limit for disconnected sessions to 60 seconds or less.

Vulnerability Key: V0018158
STIG ID: CTX0350
Release Number: 1

Status: Active
Short Name: User connection denials are not logged.
Long Name: User connection denials are not logged.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.4 Reporting
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0350
Severity: Category II
Long Name: User connection denials are not logged.
Vulnerability Discussion: Recording denied user connections will provide an audit trail for administrators to review at a later time. Denied connections might be a sign of an attacker trying to gain access to the network. By default, this type of event logging is disabled. Event logging records an entry in the System log each time a server denies a user connection because of a connection control limit. Each server records the data in its"□ own System log.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0350 (Manual)

Access the XenApp server and perform the following:
1. Select a farm in the scope pane of the Access Management Console and select Action > Modify farm properties > Modify all properties.
2. Open the Connection Limits page in the farm"□s Properties list.
3. Verify that the "Log over-the-limit denials"□ is checked. If it is not, this is a finding.

Fixes: CTX0350 (Manual)

Log all denied connections to the XenApp server"□s system log.

Vulnerability Key: V0018159
STIG ID: CTX0360
Release Number: 1
Status: Active
Short Name: Administrative tasks are not logged to database.
Long Name: XenApp farm is not logging administrative tasks to the logging database.
IA Controls: ECAR-1 Audit Record Content

ECAR-2 Audit Record Content
ECAR-3 Audit Record Content

Categories: 10.4 Reporting

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0360

Severity: Category II

Long Name: XenApp farm is not logging administrative tasks to the logging database.

Vulnerability Discussion: The Configuration Logging feature allows the tracking of administrative changes made to the server farm environment. For configuration logging to work, the site has to be using Microsoft SQL 2005/Express or Oracle databases. Reports may be generated via Configuration Logging making it possible to determine what changes were made to the server farm, when they were made, and which administrators made them. This is especially useful when multiple administrators are modifying the configuration of the server farm. It also facilitates the identification and, if necessary, reversion of administrative changes that may be causing problems for the server farm.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0360 (Manual)

For configuration logging to work, the site has to be using Microsoft SQL 2005/Express or Oracle databases.
Access the XenApp server and perform the following:
1. Select a farm in the scope pane of the Access Management Console and
select Action > Modify farm properties > Modify all properties.
2. Open the Configuration Logging page in the farm"□s Properties list.
3. Verify that the "Log administrative tasks to logging database"□ is checked. If it is not, this is a finding.

If the site is not using Microsoft SQL 2005/Express or Oracle databases, the configuration logging functionality will not be enabled. If this is the case, the IAO must provide an acceptance of risk document. If there is no document, this is a finding.

Fixes:

CTX0360 (Manual)

Enable logging of administrative tasks for the server farm or have a signed acceptance of risk document for sites that do not use Microsoft SQL 2005/Express or Oracle databases.

Vulnerability Key: V0018160

STIG ID: CTX0370

Release Number: 1

Status: Active
Short Name: Administrator actions not logged to database.
Long Name: XenApp farm is configured to allow administrator to change farm settings when the database is disconnected.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.4 Reporting
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0370
Severity: Category II
Long Name: XenApp farm is configured to allow administrator to change farm settings when the database is disconnected.
Vulnerability Discussion: Configuration Logging provides the option of allowing administrators to make changes when the database is disconnected. If changes are allowed when the database is disconnected, then administrator activity will not be logged and auditing will be impossible. Therefore, administrators will not be able to make changes unless the log entries can be saved to the database. This will provide an audit trail for review at a later date.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0370 (Manual)
Access the XenApp server and perform the following:
1. Select a farm in the scope pane of the Access Management Console and select Action > Modify farm properties > Modify all properties.
2. Open the Configuration Logging page in the farm"□s Properties list.
3. Verify that the "Allow changes to the farm when the database is disconnected"□ is not checked. If
it is checked, this is a finding.
Fixes: CTX0370 (Manual)
Disable farm setting changes when the database is disconnected.

Vulnerability Key: V0018163
STIG ID: CTX0380
Release Number: 1

Status: Active
Short Name: Credentials are not required to clean log.
Long Name: XenApp administrators do not enter credentials before cleaning the log.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 1.3 Identity Management
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0380
Severity: Category III
Long Name: XenApp administrators do not enter credentials before cleaning the log.
Vulnerability Discussion: The Configuration Logging feature allows the tracking of administrative changes made to the server farm environment. Reports may be generated that can determine what changes were made on the server farm, when they were made, and which administrator made them. This is useful when multiple administrators are modifying the configuration of your server farm. It also facilitates the identification and, if necessary, reversion of administrative changes that may be causing problems for the server farm. To manage which database users can clear the configuration log, Citrix recommends that you enable the "require administrators to enter database credentials before clearing the log"□ check box. This ensures only database users with permissions to clear the logs can clear them. Therefore, anyone attempting to use the Clearing the Log option will be prompted for database credentials.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0380 (Manual)

If Check CTX0360 is a finding, this is a finding. If CTX360 is not a finding, access the XenApp server and perform the following:
1. Select a farm in the scope pane of the Access Management Console and select Action > Modify farm properties > Modify all properties.
2. Open the Configuration Logging page in the farm"□s Properties list.
3. Verify that the "Require administrators to enter database credentials before cleaning the log"□ is checked. If it is unchecked, this is a finding.

Fixes: CTX0380 (Manual)

Require administrators to enter credentials before cleaning logs.

Vulnerability Key: V0018169

STIG ID: CTX0390
Release Number: 1
Status: Active
Short Name: Remote console connections are not disabled.
Long Name: Remote console connections are not disabled on XenApp Servers.
IA Controls: EBRP-1 Remote Access for Privileged Functions
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0390
Severity: Category I
Long Name: Remote console connections are not disabled on XenApp Servers.
Vulnerability Discussion: XenApp provides the ability to remotely manage the XenApp Servers through the remote console (Access Management or Presentation Server Console). Using the remote console defeats the security purpose of the XenApp Server Access Management or Presentation Server Console. If the remote console is used, it directs console capability to wherever the remote console is defined. Administration actions on the entire XenApp farm may be initiated without the knowledge of local conditions, and potentially compromise privileged information or deny service to the user community. The XenApp remote console is not necessary and provides another attack vector if enabled. RDP may be used to access the XenApp Server as well as other third party tools.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0390 (Manual)

Access the XenApp server and perform the following:
1. Select a farm in the scope pane of the Access Management Console and select Action > Modify farm properties > Modify all properties.
2. From the Properties list, select Server Default > XenApp. Select the Remote Console Connections page.
3. Verify that the "Remote connections to the console"□ is NOT checked. If it is checked, this is a finding.

Fixes: CTX0390 (Manual)

Disable remote console access to the XenApp farm.

Vulnerability Key: V0018170
STIG ID: CTX0400

Release Number: 1
Status: Active
Short Name: ICA TCP disconnected sessions are not reset.
Long Name: ICA TCP sessions are not configured to reset disconnected sessions.
IA Controls: EBRP-1 Remote Access for Privileged Functions
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0400
Severity: Category II
Long Name: ICA TCP sessions are not configured to reset disconnected sessions.
Vulnerability Discussion: By default, the ICA TCP connection on a computer running Citrix XenApp server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by the Citrix XenApp Client within the 60 second limit. The connection can be configured to reset, or log off, sessions with broken or timed out connections. When a session is reset, attempting to reconnect initiates a new session; rather than restoring a user to the same place in the application in use, the application is restarted. If the XenApp Server is configured to reset sessions, Auto Client Reconnect creates a new session. This process requires users to enter their credentials to log on to the server. If disconnected sessions are not disconnected, there is a chance that an authorized user may gain access to the open session.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0400 (Manual)

Access the XenApp farm and perform the following:
1. Select Start > All Programs > Administrative Tools > Terminal Services Configuration
2. Select ICA-tcp > Sessions Tab
3. Verify that the "Override user settings"□ is selected and "End Session"□ is selected. If not, this is a finding.

Fixes: CTX0400 (Manual)

Reset all ICA-tcp disconnected sessions.

Vulnerability Key: V0018171
STIG ID: CTX0410
Release Number: 3

Status: Active
Short Name: Auto-client reconnect has no authentication.
Long Name: Auto-client reconnect does not require 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 Server (Target: XenApp Server)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: CTX0410
Severity: Category II
Long Name: Auto-client reconnect does not require authentication.
Vulnerability Discussion: Users can be disconnected from their ICA sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the auto-client reconnection feature, the client can detect unintended disconnections of ICA sessions and automatically reconnect users to the affected sessions. When this feature is enabled on a computer running Citrix XenApp Server, users do not have to reconnect manually to continue working. The client attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. Requiring user authentication before reconnecting the session ensures an unauthorized user doesn"□t gain access to the session. If user authentication is required, a dialog box requesting credentials is displayed to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off. Users can only reconnect to disconnected sessions.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0410 (Manual)

Access the XenApp server and perform the following:
1. Start >Run > and type "cmd"□, enter
2. At the command prompt, type the following:
C:\>acrcfg /query
Auto Client Reconnect Info for: Local Server
INHERIT: off
REQUIRE: off
LOGGING: off

If REQUIRE: off and INHERIT: off is set, this is a finding. If REQUIRE is set to "on"□, then users are prompted for credentials during automatic reconnection. This would not be a finding.

Caveat: Servers may have INHERIT: on, and REQUIRE: off. If so, then check the farm by performing the following:

C:\>acrcfg /farm name /query

Auto Client Reconnect Info for: (farm name)
INHERIT: off
REQUIRE: on
LOGGING: off

Verify that REQUIRE is set to "on". If not, this is a finding.

Fixes: CTX0410 (Manual)

Access the XenApp server and perform the following:
1. Start > Run > and type "cmd", enter
2. At the command prompt, type the following:

C:\>acrcfg /server:servername /require:on

3. The other option is to configure these parameters on the farm by peforming the following:

C:\>acrcfg /farm /require:on

Vulnerability Key: V0018172
STIG ID: CTX0420
Release Number: 2
Status: Active
Short Name: ICA reconnection events are not logged.
Long Name: ICA reconnection events are not logged.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.4 Reporting
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0420
Severity: Category II
Long Name: ICA reconnection events are not logged.
Vulnerability Discussion: Reconnection logging is disabled by default. When logging is enabled, the XenApp server"s system log captures information about successful and failed automatic reconnection events to help with diagnosis of network problems. Automatic reconnection can fail if the client submits

incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection. Each server stores information about reconnection events in its own System log. Logging these events is important so that administrators may review failed logins to ensure no unusual activity is occurring.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0420 (Manual)

If CTX0410 is satisfied, this is not a finding.

Access the XenApp server and perform the following:
1. Start >Run >and type "cmd"□, enter
2. At the command prompt, type the following:
C:\>acrcfg /query
Auto Client Reconnect Info for: Local Server
INHERIT: off
REQUIRE: off
LOGGING: off
If logging is set to "off"□, this is a finding.

Fixes:

CTX0420 (Manual)

Access the XenApp server and perform the following:
1. Start > Run > and type "cmd"□, enter
2. At the command prompt, type the following:

C:\>acrcfg /server:servername /logging:on

Vulnerability Key: V0018173
STIG ID: CTX0430
Release Number: 3
Status: Active
Short Name: Terminal Services are not configured for XenApp
Long Name: Terminal Services are not configured correctly for XenApp.
IA Controls: EBRP-1 Remote Access for Privileged Functions
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

	☑	☑	☑

STIG ID: CTX0430

Severity: Category II

Long Name: Terminal Services are not configured correctly for XenApp.

Vulnerability Discussion: Terminal Services / Remote Desktop Services (TS/RDS) is a service that allows users to connect to a remote Microsoft Windows computer. TS/RDS allows users of virtually any device to be able to access the same application and data from anywhere. All applications and code execute exclusively on the terminal servers, allowing devices to execute the latest and most feature-rich applications, even if the device would not natively support these applications. The terminal servers present the user interface to the user□s device. The end user interacts with this interface via the keyboard and mouse, transmitting these signals to the terminal servers. TS/RDS rules from the Windows Server OS STIGs lock down several settings which would cause XenApp to not function properly. To ensure that XenApp functions properly, several TS/RDS requirements are not applicable. The requirements in the Windows Server 2003, 2008, and 2008 R2 STIGs that are not applicable are V-1112 and V-3449. V-3449 restricts terminal service users to one session. This setting would prevent running two or more published applications from running on the same XenApp server. V-1112 disables dormant user accounts on the system. There are two accounts required for XenApp to function, Ctx_configMgr and Ctx_cpuuser. However, Citrix accounts would be considered valid exceptions under the current conditions - application accounts. V-3450 from the Windows Server 2003 STIG is also not applicable. V-3450 limits the number of simultaneous connections allowed to the terminal server. This limit to one connection is not necessary since Citrix Load Balancer and policies will be used to enforce the number of connections.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0430 (Manual)

On the XenApp server perform the following:
Work with the system administrator and Windows reviewer to determine whether these are a finding.
1. Select Start > Run
2. Type "regedit"
3. Navigate to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\
4. V-3449: Verify fSingleSessionPerUser is set to 0. If not this is a finding.
5. V-3450 (Windows 2003 Server only): Verify MaxInstanceCount is set to 999999 or Not Configured/Disabled. If not, this is a finding.
6. V-1112: Using the DUMPSEC utility: Select □Dump Users as Table□ from the □Report□ menu. Select the available fields in the following sequence, and click on the □Add□ button for each entry: UserName SID PswdRequired PswdExpires PswdLastSetTime LastLogonTime AcctDisabled Groups. If any enabled accounts have not been logged into within the past 35 days, this is a finding. This can be ascertained by examining the time in the □LastLogonTime□ column. The two accounts that are required for XenApp to function are the Ctx_configMgr and Ctx_cpuuser. These accounts will be exempt from this check.

Fixes: CTX0430 (Manual)

Disable the Terminal Services requirements that are not applicable to XenApp Servers.

Vulnerability Key: V0018175

STIG ID: CTX0450

Release Number: 1

Status: Active

Short Name: ICA-TCP permissions are not documented.

Long Name: The ICA-TCP user and group permissions are not documented.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 2.1 Object Permissions

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0450

Severity: Category III

Long Name: The ICA-TCP user and group permissions are not documented.

Vulnerability Discussion: An ICA session is the communication link between clients and servers that users establish to run applications, which is very similar to an RDP session. An ICA session transmits an application"□s screen display to the client and the client sends the user"□s keystrokes, mouse actions, and local data to the application running on the server. The default users and groups for the ICA-tcp protocol are the following: Administrators Ctx_cpsvcuser Local Service Network Service Remote Desktop Users System Permissions need to be documented and verified to ensure unauthorized users do not gain access to published applications.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0450 (Manual)

1. Request the ICA-tcp permissions document from the IAO/SA. If no document can be produced, this is a finding.
2. Access the Citrix XenApp server, select Start > All Programs > Administrative Tools > Terminal Services Configuration.
3. Right-click the ICA-tcp Connection, select the permissions tab, and verify the users and group permissions match the documentation. If not, this is finding.

Fixes: CTX0450 (Manual)

Document the ICA-tcp user and group permissions.

Vulnerability Key: V0018345

STIG ID: CTX0460

Release Number: 1

Status: Active

Short Name: IMA encryption is disabled for XenApp farm.

Long Name: Independent Management Architecture (IMA) encryption is disabled for the XenApp farm.

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

Categories: 8.2 Encrypted Data at Rest

Effective Date: 29 Jun 2009

	Comments:

☐ Open ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0460

Severity: Category II

Long Name: Independent Management Architecture (IMA) encryption is disabled for the XenApp farm.

Vulnerability Discussion: Independent Management Architecture (IMA) is the underlying architecture used in Citrix XenApp server for configuring, monitoring, and operating all XenApp server functions. The IMA data store stores all XenApp server configurations. Items that are stored in the IMA Data store include published applications, administrator names, permissions, and server listings. IMA encryption is a farm-wide setting that applies to all servers in the farm once it is enabled. The IMA encryption feature protects administrative and sensitive data that is stored in the IMA data store database. Encryption also ensures that Citrix administrators are not able to access the configuration logging database and enforces strict separation of duties.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0460 (Manual)

Access the XenApp server and perform the following:
1. Select Start > Run > and type "cmd"□.
2. At the command prompt, type the following:
C:\>:ctxkeytool query

If IMA encryption is not enabled, this is a finding. If no key exists, this is a finding. (farmkey.ctx is the default key that is created, but this may be changed during installation. Make sure that a key file exists to ensure compliance.)

Fixes:

CTX0460 (Manual)

Generate a new key for the Citrix Farm by performing the following:
1. On the server on which you want to enable IMA encryption, run the generate option of the ctxkeytool command. The following is an example of the command line to use to accomplish this: C:\>ctxkeytool generate (full UNC or absolute path, including the file name of the key you want to generate, to the location where you want to store the key file)
2. Citrix suggests naming the key after the farm it will be used on. For example, farmakey.ctx. Citrix also suggests saving the key to a folder that uses the name of your farm. For example, Farm_A_Key.
3. Press Enter. The following message appears indicating that you successfully generated a key file for that server, "Key successfully generated."□
4. Run the newkey option of the ctxkeytool command to use the currently loaded key and enable the key. For instance, C:\>ctxkeytool newkey
5. Press Enter. The following message appears indicating that you successfully enabled the IMA encryption feature in the data store, "The key for this farm has been replaced. IMA Encryption is enabled for this farm."□

Vulnerability Key: V0018181
STIG ID: CTX0470
Release Number: 1
Status: Active
Short Name: The XenApp farm does not have unique IMA keys.
Long Name: The Citrix XenApp farm does not have unique IMA keys.
IA Controls: IAKM-1 Key Management
IAKM-2 Key Management
IAKM-3 Key Management
Categories: 8.4 Key Management
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0470
Severity: Category II
Long Name: The Citrix XenApp farm does not have unique IMA keys.
Vulnerability Discussion: The IMA encryption feature protects administrative and sensitive data stored in the IMA data store. Enabling IMA encryption provides a higher degree of security for the configuration logging feature. The IMA key that is generated enables the encryption. If the same key is used for all XenApp farms, a compromise of one farm would allow access to the data on all the XenApp farms.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0470 (Manual)

If only one XenApp Farm exists, this check is not applicable.
If multiple XenApp Farms exist, then select Start > Run, and type "cmd"□.
1. At the command prompt, type the following: C:\>ctxkeytool query
2. If the IMA key is the same as the other Citrix Farm key, this is a finding.
(farmkey.ctx is the file that needs to be present)

Fixes: CTX0470 (Manual)

Generate a new key for the Citrix Farm by performing the following:
1. On the server on which you want to enable IMA encryption, run the generate option of the ctxkeytool command. The following is an example of the command line to use to accomplish this: C:\>ctxkeytool generate (full UNC or absolute path, including the file name of the key you want to generate, to the location where you want to store the key file)
2. Citrix suggests naming the key after the farm it will be used on. For example, farmakey.ctx. Citrix also suggests saving the key to a folder that uses the name of your farm. For example, Farm_A_Key.
3. Press Enter. The following message appears indicating that you successfully generated a key file for that server, "Key successfully generated."□

4. Run the newkey option of the ctxkeytool command to use the currently loaded key and enable the key. For instance, C:\>ctxkeytool newkey
5. Press Enter. The following message appears indicating that you successfully enabled the IMA encryption feature in the data store, "The key for this farm has been replaced. IMA Encryption is enabled for this farm."

Vulnerability Key: V0018182
STIG ID: CTX0480
Release Number: 1
Status: Active
Short Name: IMA keys are not restricted to unauthorized users.
Long Name: The IAO/SA will restrict access to the IMA key to only authorized personnel. These users will be documented and listed in the Read/Execute access permissions.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.1 Object Permissions
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0480
Severity: Category II
Long Name: The IAO/SA will restrict access to the IMA key to only authorized personnel. These users will be documented and listed in the Read/Execute access permissions.
Vulnerability Discussion: IMA encryption is a farm-wide setting that applies to all servers in the farm once it is enabled. The IMA encryption feature protects administrative and sensitive data that is stored in the IMA data store database. Encryption also ensures that Citrix administrators are not able to access the configuration logging database and enforces strict separation of duties. The IMA key that is generated enables the encryption. Restricting access to the IMA key will ensure unauthorized users are not able to use the key and access the IMA data store database.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0480 (Manual)

1. Ask the IAO/SA where the IMA key is located on the network. Request the permission documentation from the IAO/SA for the IMA key.
2. Access the folder where the IMA key is located and view the permissions and rights on this folder. Verify that Read and Execute permissions are restricted to authorized users only for each XenApp Server.

3. Compare the actual permission configuration with the documented permissions. If any discrepancy exists, this is a finding.

Fixes: CTX0480 (Manual)
Restrict access to IMA keys to authorized users only and document authorized users.

Vulnerability Key: V0018200
STIG ID: CTX0510
Release Number: 1
Status: Active
Short Name: Anonymous users are enabled.
Long Name: Anonymous users are enabled for published applications.
IA Controls: ECPA-1 Privileged Account Control
Categories: 1.4 Authentication Services
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0510
Severity: Category II
Long Name: Anonymous users are enabled for published applications.
Vulnerability Discussion: When XenApp is installed a special group named Anonymous is created which by default contains 15 user accounts with names in the form of AnonXXX, where XXX is a number from 000 to 014. These anonymous users have guest permissions and differ from other user accounts in that they have a default 10 minute idle time before being logged off. Anonymous accounts also have no password requirement. Published resources will be required to authenticate users, and these anonymous accounts will be deleted to ensure unauthorized users may not login to the XenApp farm.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0510 (Manual)

Access the XenApp server and perform the following:
1. Select Start > All Programs > Administrative Tools > Computer Management
2. On the left hand side, select Local Users and Groups > Users
3. Verify that all Anon000 thru Anon014 are deleted. If they are disabled or enabled, this is a finding. Disabled User icons have a red "x" through the face. If the users are not present (i.e., deleted from system), this is not a finding.

Fixes: CTX0510 (Manual)
Delete all anonymous users accounts (Anon000 thru Anon014) on all XenApp servers.

Vulnerability Key: V0018201
STIG ID: CTX0520
Release Number: 1
Status: Active
Short Name: XenApp server has disabled isolation environments.
Long Name: XenApp server has disabled isolation environments.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0520
Severity: Category III
Long Name: XenApp server has disabled isolation environments.
Vulnerability Discussion: Enterprise applications published using Citrix XenApp Server often share specific operating system resources. Such sharing enables efficient use of limited system resources. However, sharing of system resources also introduces interdependencies between applications which, in turn, introduce compatibility issues in a multi-user environment. For example, a simple software patch applied to a particular application could affect another application that depends on a shared component. The two applications could subsequently begin to misbehave or fail. The isolation environment protects the operating system and applications from conflicts and other complications that frequently occur between incompatible or legacy applications. The isolation environment creates an environment or user specific copy of the system resources modified by the published application during installation or runtime. This allows the application to function without affecting the rest of the system. Creating isolation environments on farms enables safe installation and execution of applications. It also mitigates application compatibility issues in a server environment.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0520 (Manual)

To verify isolation environments are enabled for a farm and/or XenApp servers, perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console.
2. Select the farm in the scope pane of the Access Management Console and right click on the farm. Select Modify farm properties > Modify all properties.

3. Navigate to Server Default > Isolation Environment page in the farm"□s Properties list.
4. Check to see if the "Application isolation"□ check box is selected. If it is not selected, this means that Application isolation is disabled for the farm. If it is selected, this means Application isolation is enabled for the farm.
5. Select the server in the scope pane of the Access Management Console and right click on the server. Select Modify server properties > Modify all properties.
6. Select the Isolation Environment page in the server"□s Properties list
7. If the "Use farm settings"□ is selected, then refer to the results in the Isolation Environment page for the farm"□s properties list in step 4. If Step 4 had "Application isolation"□ enabled, this is not a finding. If Farm's Properties list in Step 4 had "Application isolation"□ disabled, then proceed to step 8.
8. Within the Isolation Evironment page in the server's properties list, verify that the "Application isolation"□ is selected. If it is selected, this is not a finding. If it is not selected, this is a finding.

Caveat: If server resources are limited on the XenApp server, CTX0520 may cause performance issues. CTX0520 may be marked Not a Finding if there is written documentation stating that CTX0520 will cause performance issues on the XenApp server.

Fixes: CTX0520 (Manual)
Enable isolation environments for the XenApp server.

Vulnerability Key: V0018202
STIG ID: CTX0530
Release Number: 1
Status: Active
Short Name: Isolation environment has no enhanced security.
Long Name: Isolation environment is not configured with enhanced security.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0530
Severity: Category III
Long Name: Isolation environment is not configured with enhanced security.
Vulnerability Discussion: Isolation environment may have two types of security, enhanced or relaxed. Enhanced security prevents users connected to isolated applications from executing files (such as .exe, .dll, and .ocx) located in the server hard drive folders created under the user profile root when the user logs on. This security level prevents issues caused by running files that could cause application

conflicts, hijack DLLs, or install hostile code on the system. Relaxed security allows users in isolation environments to download executable files into the user profile root, as well as installation root or in the actual physical location. User profile root enables the isolation environment to create and maintain profile-specific copies of the files modified by the user. The user profile root is a unique folder created for each user profile. User profile root captures all changes made by a user during application execution within a user session and prevents an application which is incompatible in a Terminal Service environment from causing conflicts when accessed by multiple users. User profile root also enables tracking of files which were deleted for a particular user of an isolation environment. Actual files are not deleted, only virtual files from the user profile root. This enhances file and server security since users are "sandboxed" when accessing published applications.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0530 (Manual)

If CTX0520 is a finding, this will be a finding as well.
1. Select Start > All Programs > Citrix > Management Consoles > Presentation Server Console
2. In the left pane of the Presentation Server Console, select the Isolation Environments node.
3. Right Click on the Applications that are configured for Isolation Environments and select Properties.
4. Select the Security Option and verify that "Enhanced security" is selected. If so, this is not a finding. If "Relaxed security" is selected, this is a finding.
5. Perform these above steps for all applications listed.

Caveat: If server resources are limited on the XenApp server, CTX0530 may cause performance issues.

Fixes: CTX0530 (Manual)

Configure all isolation environments to use enhanced security.

Vulnerability Key: V0018203
STIG ID: CTX0540
Release Number: 1
Status: Active
Short Name: Client mapped drives are set to "execute" permiss.
Long Name: Client mapped drives are configured with "execute" permissions on the XenApp server.
IA Controls: ECCD-1 Changes to Data
Categories: 2.1 Object Permissions
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

Public	☑	☑	☑

STIG ID: CTX0540

Severity: Category II

Long Name: Client mapped drives are configured with "execute" permissions on the XenApp server.

Vulnerability Discussion: Client drive mappings are built into the standard device redirection facilities of the Citrix XenApp Server. The client drives appear as client network objects in Windows. The client"s disk drives are displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive. Client drive mappings pose a security risk because they allow the client to read and write from their local drives files to the XenApp server This allows users to transfer rogue files onto the server that could contain malware or malicious code. Transferring files from client devices to the XenApp server may use up disk space or infect the server with a virus that could affect the availability and integrity of the XenApp server. If client drive mappings is enabled, the server maps client drives without user execute permission. For users to be able to execute files residing on mapped client drives, this setting must be changed by editing the value of ExecuteFromMappedDrive in the registry on a server running Citrix XenApp. Running client programs on the server may unintentionally cause issues with the Citrix XenApp server and potentially cause a denial of service.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0540 (Manual)

To verify the "execute" permissions is off for client drives, perform the following on the XenApp server:
1. Select Start > Run
2. Type "regedit" and press enter.
2. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdm\Parameters\ExecuteFromMappedDrive
3. Verify that the ExecuteFromMappedDrive is set to 0. If it is not set to 0, this is a finding.
Setting this registry key to 0 denies users execute permission on mapped drives.

Fixes:

CTX0540 (Manual)

Disable "execute" permission on client mapped drives via the registry on the XenApp Server.

Vulnerability Key: V0018204

STIG ID: CTX0550

Release Number: 1

Status: Active

Short Name: XenApp servers are not configured with monitoring

Long Name: XenApp servers are not configured with monitoring alerts.

IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

Categories: 12.4 CM Process

Effective Date: 29 Jun 2009

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

Condition:

XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0550

Severity: Category II

Long Name: XenApp servers are not configured with monitoring alerts.

Vulnerability Discussion: Health Monitoring & Recovery is a feature that is available only with the Enterprise Edition of Citrix Presentation Server. The Health Monitoring & Recovery feature can run tests on servers in a server farm to monitor states and discover any health risks. Without an on-line monitoring system in place, unusual or inappropriate activity will could go unnoticed or without detection. Activity could include system services stopping or starting, file changes, and so on. These changes may happen before the system administrator has time to review any logs.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0550 (Manual)

If the Citrix XenApp Enterprise Edition is used for monitoring processes, verify the following tests are configured on the XenApp server:
1. Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Select the Farm > Modify server properties > Modify all properties
3. Navigate to Server Default > Health Monitoring & Recovery
4. Verify that "Run health check tests on all servers in the farm"□ is checked. If it is not, this is a finding.

If the site is using a third party tool, verify the following service tests are configured:
1. Citrix IMA Service test
2. Logon Monitor test
3. Terminal Services test
4. XML Service test.

If these services are not monitored, this is a finding.

Fixes:

CTX0550 (Manual)

Configure monitoring alerts on all XenApp servers.

Vulnerability Key: V0018206

STIG ID: CTX0570

Release Number: 2

Status: Active

Short Name: Unauthorized users have access to the LHC.

Long Name: Unauthorized users have access to the Local Host Cache database.

IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data

Categories: 2.1 Object Permissions

Effective Date: 29 Jun 2009

☐ Open	Comments:

☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0570

Severity: Category II

Long Name: Unauthorized users have access to the Local Host Cache database.

Vulnerability Discussion: The Local Host Cache (LHC) is a partial copy of the data store database that every XenApp Server maintains locally to the server itself. The partial local replica is maintained in MS Access format and is encrypted, similar to the information in the data store database. The LHC allows the XenApp Server to continue running based on the configuration that was last received from the data store, if the data store is unavailable. Secondly, the LHC increases performance by reducing bottlenecks at the server housing the data store , providing much greater scalability. The LHC database is located at C:\Program Files\Citrix\Independent Management Architecture in a file named MF20.mdb (MS Access) or IMALHC.mdb. XenApp administrators and users cannot directly query or change the information in the data store since it is in a binary format. However, it is possible that someone with database administrative rights could delete portions of the database. Therefore, permissions to this database need to be restricted and monitored.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0570 (Manual)

Ensure only the required users have NTFS permissions to the MF20.mdb (MS Access) or IMALHC.mdb file.
1. Access the permissions on the MF20.mdb or IMALHC.mdb file by navigating to the C:\Program Files\Citrix\Independent Management Architecture. If the MF20.mdb or IMALHC.mdb files are not at this location, then select Start > Search > Files and Folders and type in MF20.mdb or IMALHC.mdb.
2. Right click on the file and select the Security tab.
3. Verify the following users have access to the MF20.mdb and IMALHC.mdb file:

Administrators
System

4. For the SQL IMALHC.mdb file, verify that the NETWORK SERVICE group is present with all rights except:
DELETE, CHANGE PERMISSIONS, and TAKE OWNERSHIP.

If the NETWORK SERVICE group is not listed with the correct permissions, this is a finding.

If other users are listed in either of these files, this is a finding.

Fixes: CTX0570 (Manual)

Restrict access to the Local Host Cache file.

Vulnerability Key: V0018207
STIG ID: CTX0580
Release Number: 1
Status: Active
Short Name: ICA GPO is not configured for XenApp farm.
Long Name: ICA GPO is not configured for the XenApp farm.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0580

Severity: Category III

Long Name: ICA GPO is not configured for the XenApp farm.

Vulnerability Discussion: XenApp farms may be configured with Group Policy Objects (GPOs). If the site uses GPOs, terminal services settings in GPOs have been shown to affect both RDP and ICA protocols. Therefore, separating GPOs for terminal services and XenApp servers will provide for a more stable and available environment. For instance, using a single GPO for all terminal servers and setting the maximum time setting to 3 hours would be problematic if users needed access all day. Therefore, configure separate GPOs for remote administration and XenApp servers.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0580 (Manual)

Ask the IAO/SA if GPOs are used. If they are not, this is not a finding. If they are used, perform the following:
1. Select Start, and then click Run.
2. In the open box, type "mmc", and then click OK.
3. On the File menu, click Add/Remove Snap-in.
4. Click Add.
5. Under Available Stand-alone Snap-ins, click Group Policy, and click Add.
6. Navigate to Computer Configuration > Administrative Templates > Citrix Components > Presentation Server Client. This will verify that the ICA policies have been loaded onto the server. If these are not loaded, this is a finding.

Fixes: CTX0580 (Manual)

Configure a separate ICA GPO within Active Directory that does not include the Terminal Services GPO.

Vulnerability Key: V0018208
STIG ID: CTX0590
Release Number: 1
Status: Active
Short Name: XenApp Organizational Unit (OU) is not configured.
Long Name: XenApp Organizational Unit (OU) for clients is not configured for domain.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0590
Severity: Category III
Long Name: XenApp Organizational Unit (OU) for clients is not configured for domain.
Vulnerability Discussion: Active Directory improves scalability in large organizations through the use of organizational units (OUs). An OU is basically a collection of users and computers. Citrix recommends creating an OU named XENAPP and moving all user accounts and computer objects for the XenApp domain into this OU. Group policy will then be applied to this OU for the XenApp farm. Any potential group policy conflicts will be minimized by this configuration.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0590 (Manual)
Ask the IAO/SA if a separate OU has been configured for the XenApp users and computers. Access the Active Directory Users and Groups utility on the domain controller or XenApp server and verify that an OU exists for the XenApp farm. If not, this is a finding.
Fixes: CTX0590 (Manual)
Configure a separate OU for XenApp servers and clients within the domain.

Vulnerability Key: V0018209
STIG ID: CTX0600
Release Number: 3
Status: Active
Short Name: Permissions are not configured for applications.
Long Name: Permissions are not configured for users accessing published applications.
IA Controls: ECCD-1 Changes to Data

ECCD-2 Changes to Data

Categories: 2.1 Object Permissions

Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0600

Severity: Category II

Long Name: Permissions are not configured for users accessing published applications.

Vulnerability Discussion: Users accessing published applications may be restricted to only those published applications by configuring NTFS security on executables. Using NTFS-level security ensures that the access restriction cannot be circumvented. With NTFS security the application will not run unless the user has rights to the application.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0600 (Manual)

Access the XenApp server and perform the following:
1. Open Windows Explorer and navigate to the published application executable. For instance, C:\Windows\system32\notepad.exe. Select notepad.exe and right click on it and select Properties.
2. Select the Security tab.
3. Verify that only authorized users or groups are listed and documented with the IAO. Typically, the following users and groups will be listed:

SYSTEM
Administrators

Power Users - contains Ctx_ConfigMgr and ctx_cpsvcuser
Remote Desktop Users or Citrix Users - contains Terminal Service users.

If users or groups are listed that are not documented with the IAO, this is a finding.

Fixes: CTX0600 (Manual)

Restrict access to published applications through the use of NTFS security and document authorized users and groups.

Vulnerability Key: V0018210

STIG ID: CTX0610

Release Number: 2

Status: Active

Short Name: Management console executables are not restricted.
Long Name: Management console executables are not restricted to XenApp administrators only.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.1 Object Permissions
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0610
Severity: Category II
Long Name: Management console executables are not restricted to XenApp administrators only.
Vulnerability Discussion: The management console executables (ctxload.exe and CmiLaunch.exe) should be restricted to only authorized users through NTFS security. This will ensure that only authorized users can execute the console and make changes to the XenApp server or farm. Failure to restrict access to these executables could provide access to unauthorized users and allow modifications to the farm. The XenApp Server Console can be used to connect to any server in your farm.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0610 (Manual)

Access the XenApp server and perform the following:
1. Open Windows Explorer and navigate to C:\Program Files\Citrix\Administration. If the ctxload.exe file is not at this location, then select Start > Search > Files and Folders and type in ctxload.exe.
2. Select ctxload.exe and right click on it and select Properties.
3. Select the Security tab.
4. Verify only authorized groups and users are listed. These authorized users will be documented with the IAO. Typically, XenApp Administrators, Network Service, Local Server and System groups are listed. If other users or groups are listed and not documented with the IAO, this is a finding. If Network Service and Local Service have more than READ access, this is a finding.

5. Navigate to C:\Program Files\Common Files\Citrix\Access Management Console - Framework. If the CMiLaunch.exe file is not at this location, then select Start > Search > Files and Folders and type in CmiLaunch.exe.
6. Select CmiLaunch.exe and right click on it and select Properties.
7. Select the Security tab.
8. Verify only authorized groups and users are listed. These authorized users will be documented with the IAO. Typically, XenApp Administrators, System, Network Service, and Local Service groups are listed. If other users or groups are listed and not documented with the IAO, this is a finding.
If Network Service and Local Service have more than READ access, this is a finding.

Fixes: CTX0610 (Manual)

Restrict access to management consoles with NTFS security and authorized users and groups are documented.

Vulnerability Key: V0018211
STIG ID: CTX0620
Release Number: 1
Status: Active
Short Name: XenApp servers are located in the DMZ.
Long Name: XenApp servers are located in the DMZ or screened subnet.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 14.2 Protocol Security
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0620

Severity: Category II

Long Name: XenApp servers are located in the DMZ or screened subnet.

Vulnerability Discussion: If the XenApp server is configured to service clients outside the enclave, there is a potential that an external adversary can obtain information about internal XenApp servers that could assist the adversary in an attack. Firewalls, ACLs, and DMZs are used to enforce restrictions and are components in the defense-in-depth architecture. The Secure Gateway eases firewall traversal and provides a secure gateway between Citrix XenApp Server and client devices. All data traversing outside the enclave between a remote workstation and the Secure Gateway is encrypted using the Transport Layer Security (TLS) protocol. The Secure Gateway transparently encrypts and authenticates all user connections to protect against eavesdropping and data tampering. The Secure Gateway is installed in a network"□s demilitarized zone (DMZ) to form a secure perimeter around the Citrix components in the enterprise network. The Secure Gateway authenticates users connecting to the XenApp farm, and establishes a secure channel for data exchange between the client device and the Citrix XenApp Server. The Secure Gateway is an application that runs as a service on a server that is deployed in the DMZ. The server running the Secure Gateway represents a single point of access to the secure, enterprise network. The Secure Gateway acts as an intermediary for every connection request originating from outside the enclave to the enterprise network. The Secure Gateway works with components of XenApp server for logon and authentication. These include the Web Interface, Secure Ticket Authority (STA), Citrix XML Service, and Web Client. 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.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0620 (Manual)

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 XenApp servers. Access the XenApp server and type the following at the command prompt:

C:\>ipconfig /all

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

2. If the IP address is on the same network as the firewall DMZ interface, it may be a secure gateway server or Web Interface server. If it is not a secure gateway server or Web Interface server, 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: CTX0620 (Manual)

Place all XenApp servers in the enclave, not in the DMZ or screened subnet.

Vulnerability Key: V0018212
STIG ID: CTX0630
Release Number: 1
Status: Active
Short Name: The XenApp software version is not supported.
Long Name: The Citrix XenApp software version is not supported.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.8 Unsupported Vendor Products
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0630

Severity: Category I

Long Name: The Citrix XenApp software version is not supported.

Vulnerability Discussion: XenApp servers require support for release versions. The XenApp server will be a supported release to ensure the release may be patched. This will ensure the ability to comply with IAVM requirements as well as access to vendor recommended and security patches.

Responsibility: System Administrator

Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0630 (Manual)

1. To determine the XenApp or Presentation Server version, perform the following:
a. Select Start > Run
b. Type "regedit" in the box.
In the Windows Registry, navigate to the following to identify the version of XenApp server running:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

Product Build	3600
Product Name	Citrix Presentation Server
ProductVersion	4.11
NewProductVersion	4.5

The data in the "NewProductVersion" field is the version.

An alternative method to check this is to perform the following:

a. Select a farm in the scope pane of the Access Management Console and
Navigate to the XenApp farm > Servers
b. Select the appropriate server and right click on it. Select Information from the drop down menu.
c. The Information section will have the Product and Version information displayed.

2. If you have access to the internet, proceed to www.citrix.com and navigate to Support > Product Lifecycle support > Product Matrix Table. It should look similar to the table below. If you do not have access to the Internet, use this table below.

Presentation Server Model	Version/ Language	NSC	EOS	EOM	EOL
Presentation Server Standard Edition	All	EN, DE, FR, ES, JA	12-Feb-07	15-May-07	30-Jun-09
Presentation Server for Windows	4.0	EN, DE, FR, ES, JA	12-Feb-07	N/A	30-Jun-09
Presentation Server for Unix***	4.0	EN	16-Jul-08	N/A	Not Announced at this time
Presentation Server for Windows****	4.5	EN, DE, FR, ES, JA	16-Jul-08	N/A	31-Mar-11

NSC = Notice of change status
EOS = End of Sale
EOM = End of Maintenance
EOL = End of Life.

If the EOL for the XenApp server version (step 1) has expired, this is a finding.

Fixes: CTX0630 (Manual)

Use XenApp software that is supported and under maintenance.

Vulnerability Key: V0018213
STIG ID: CTX0640
Release Number: 1
Status: Active
Short Name: XenApp server patches not tested before deployed.

Long Name: XenApp server patches are not tested before deployment to productions systems.
IA Controls: DCCT-1 Compliance Testing
Categories: 3.1 Security Patches
3.2 Operational / PM Patches
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0640
Severity: Category II
Long Name: XenApp server patches are not tested before deployment to productions systems.
Vulnerability Discussion: Organizations need to stay current with all applicable XenApp server software updates that are released from Citrix. Software updates are designed to update or fix XenApp problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics, and improving the usability or performance. XenApp Servers that do not have the latest patches or updates installed may have potential vulnerabilities that may be exploited.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0640 (Manual)

To verify hotfixes are tested before rolling out to production servers, perform the following:
1. Access the test XenApp servers and in the scope pane of the Access Management Console, select the XenApp farm > server > Hotfix Management. Review the most recent hotfix listed and compare this to the one listed on Citrix"□s website.
2. Navigate to http://support.citrix.com/ and select XenApp. Scroll down to important updates and select the latest update for XenApp. Compare this with the latest hotfix listed in the XenApp server Hotfix Management.
3. If Internet access is unavailable, mark this as Not Reviewed.

Fixes: CTX0640 (Manual)

Apply the latest patches to the XenApp server.

Vulnerability Key: V0018214
STIG ID: CTX0650
Release Number: 2
Status: Active
Short Name: XenApp service account rights are not restricted.
Long Name: XenApp service account rights are not restricted.
IA Controls: ECPA-1 Privileged Account Control

Categories: 1.3 Identity Management
Effective Date: 29 Jun 2009

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

Condition: XenApp Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0650

Severity: Category II

Long Name: XenApp service account rights are not restricted.

Vulnerability Discussion: During the installation of XenApp server, several service accounts are created depending on the version of XenApp installed. These service accounts have only the necessary permissions, group memberships, and rights needed to perform those functions. Each of these accounts has their password dynamically assigned at installation time, so changing these periodically will not affect the XenApp environment. These service accounts should not be altered as any deviation from the default set of permissions and rights may result in undesirable effects. For instance, printers may not autocreate in an ICA session or certain reporting components may not function properly.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

CTX0650 (Manual)

Access the XenApp server, and perform the following:
1. Navigate to the Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.

2. Select "Debug Programs"□ and "Increase Scheduling Priority" and view the security settings. The only user for XenApp that should be listed for these policies is ctx_cpuuser. If any other XenApp user is listed, this is a finding.

3. Select "Load and Unload device Drivers"□ and view the settings. The only XenApp account for this policy will be the ctx_cpsvcuser. If others are listed, this is a finding.

5. Select "Restore Files and directories"□ and "Replace a process level token" and view the settings. The only XenApp account for these policies will be the ctx_StreamingSvc. If others are listed, this is a finding.

6. Select "Log on as a batch job"□ and "Log on as service"□ to view the security settings. All XenApp accounts will be listed in these policies. These include Ctx_CpsvcUser, Ctx_ConfigMgr, Ctx_StreamingSvc, and Ctx_CpuUser. If these accounts are not listed, this is a finding. These are the only two policies that have all user accounts listed.

Fixes:

CTX0650 (Manual)

Restrict the rights of the default XenApp accounts to the installation defaults.

Vulnerability Key: V0018216
STIG ID: CTX0670
Release Number: 1
Status: Active
Short Name: Authorized users are not documented.
Long Name: Authorized users are not documented to access the License Server.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 1.6 Documentation and Storage
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0670
Severity: Category III
Long Name: Authorized users are not documented to access the License Server.
Vulnerability Discussion: The XenApp server farm must include a license server, which stores the license files for the Citrix products that specify the parameters for the product usage. The licensing architecture consists of the Citrix Licensing Server, the License Management Console, and the License Allocation Process. If the license files are not available to the Citrix XenApp farm, the farm will continue to operate for four days, but after that the products will not be available. This could cause a denial of service to the user community. Therefore, only authorized users will have access to the License Management Console.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0670 (Manual)

1. Request the documentation that lists the authorized users for the License Management Console. If one is not available, this is a finding.
2. Open the License Server console. From the Welcome Page, select User Administration.
3. Review the users listed and compare them to the documentation. If a discrepancy exists, this is a finding.

Fixes: CTX0670 (Manual)
Configure and document authorized users for the License Management Console.

Vulnerability Key: V0018217
STIG ID: CTX0680

Release Number: 1
Status: Active
Short Name: XenApp is not registered in VMS or database.
Long Name: The XenApp Server is not registered in VMS or vulnerability management database.
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 Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0680
Severity: Category II
Long Name: The XenApp Server is not registered in VMS or vulnerability management 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 XenApp 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: CTX0680 (Manual)

If VMS is used, then ensure the XenApp 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: CTX0680 (Manual)

Register XenApp servers in VMS or vulnerability management database.

Vulnerability Key: V0018218
STIG ID: CTX0690

Release Number: 1
Status: Active
Short Name: XenApp VMS posture is incorrect.
Long Name: The XenApp 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 Server (Target: XenApp Server)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0690
Severity: Category II
Long Name: The XenApp 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: CTX0690 (Manual)

If check CTX0680 is a finding, this should automatically be marked as a finding as well. If the assets are registered in VMS ensure the following postures are registered.
The example below shows the SQL server selected, but it could be Microsoft SQL Server 2005 Express Edition SP1, Oracle database, or IBM DB2.

Win2k3
AntiVirus
XenApp Server
Database SQL Server Database 2005 - Model
Database SQL Server Database 2005 - Master
Database SQL Server Database 2005 - MSDB
Database SQL Server Database 2005 - TempDB

If any of the postures are not registered, this is a finding.

Caveat: The IMA Data store may be on a dedicated host and the database posture will then be not applicable for the XenApp server.

Fixes: CTX0690 (Manual)

Configure all XenApp assets into VMS with the correct posture.

Vulnerability Count - 46