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 Policy

Vulnerability Key: V0017989
STIG ID: CTX0010
Release Number: 1
Status: Active
Short Name: No documentation for XenApp infrastructure
Long Name: There is no up-to-date documentation of the Citrix XenApp infrastructure.
IA Controls: DCHW-1 HW Baseline
DCSW-1 SW Baseline
Categories: 12.9 Documentation
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0010
Severity: Category III
Long Name: There is no up-to-date documentation of the Citrix XenApp infrastructure.

Vulnerability Discussion: Without current and accurate documentation, any changes to the XenApp infrastructure may jeopardize the networkâ€™s integrity. To assist in the management, auditing, and security of the network, facility drawings and topology maps are a necessity. Topology maps and documentation are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks could take place. Additionally, documentation along with diagrams of the network topology is required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0010 (Manual)

Request a copy of all the Citrix XenApp infrastructure documentation. Documentation must include all XenApp servers, Secure Gateway servers, Web Interface servers, protocols, ports, and IP addresses. If the documentation is incomplete or missing components, this is a finding.

Fixes: CTX0010 (Manual)

Develop up-to-date documentation for the Citrix XenApp infrastructure.

Vulnerability Key: V0017990
STIG ID: CTX0020
Release Number: 1
Status: Active
Short Name: No XenApp subscription to patches and hotfixes
Long Name: The IAO/SA does not subscribe to Citrix XenApp security patches and hotfix notifications.
IA Controls: ECSC-1 Security Configuration Compliance
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 Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0020
Severity: Category III
Long Name: The IAO/SA does not subscribe to Citrix XenApp security patches and hotfix notifications.
Vulnerability Discussion: Organizations need to stay current with all applicable XenApp software updates that are released from Citrix. In order to be aware of updates as they are released, system administrators will subscribe to XenApp Server vendor security notices, updates, and patches to ensure that all new vulnerabilities are known. New XenApp server and updates should be reviewed for the XenApp

server before moving them into a production environment.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0020 (Manual)

Notifications from Citrix are received through the Citrix Knowledge Centerâ€™s email alert center systems accessed through the personâ€™s MyCitrix account. Ask the IAO/SA to provide actual update notification to verify that they are on the subscription list. If no emails or documentation can be provided, this is a finding.

Fixes: CTX0020 (Manual)

Subscribe to vendor security and patch notifications.

Vulnerability Key: V0017991
STIG ID: CTX0030
Release Number: 3
Status: Active
Short Name: No XenApp images or backup procedures.
Long Name: There are no XenApp images or procedures for backup and recovery.
IA Controls: COBR-1 Protection of Backup and Restoration Assets
Categories: 13.4 Backup & Recovery
Effective Date: 29 Jun 2009

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

Condition: XenApp Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0030
Severity: Category II
Long Name: There are no XenApp images or procedures for backup and recovery.
Vulnerability Discussion: Availability of the Citrix XenApp server will be hindered if the system is compromised, shutdown, or unavailable. Backup and recovery procedures are critical to the availability and protection of the Citrix XenApp server. Personnel should be knowledgeable in the backup procedures, media location, and recovery process. Therefore, procedures are necessary for backing up and restoring Citrix XenApp Servers. In addition to the backup procedures, standard file backups are not practical or recommended for XenApp servers. Since all the XenApp data is stored on the data store database (Oracle or SQL), creating XenApp images for backup and recovery is recommended since the application files do not change, unless there is a patch or upgrade applied to the server. If patches or upgrades were applied to the servers, then new backup images would need to be created.

Responsibility: System Administrator

Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0030 (Manual)

1. Request a copy of the backup and recovery procedures for the XenApp servers, Secure Gateway servers, and Web Interface servers. If no procedures exist, this is a finding.
2. Review the location of the server images. If no server images have been created or are inaccessible, this is a finding.
Note: If patches or upgrades were applied to the servers, then new backup images would need to be created.

Fixes: CTX0030 (Manual)

Develop XenApp backup and recovery procedures. Create XenApp server images and update them when new patches are applied.

Vulnerability Key: V0017992
STIG ID: CTX0040
Release Number: 1
Status: Active
Short Name: There are no disaster recovery plans for XenApp
Long Name: There are no disaster recovery plans for the Citrix XenApp system.
IA Controls: CODP-1 Disaster and Recovery Planning
CODP-2 Disaster and Recovery Planning
CODP-3 Disaster and Recovery Planning
Categories: 13.3 Coop Plans
Effective Date: 29 Jun 2009

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

Condition: XenApp Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0040
Severity: Category II
Long Name: There are no disaster recovery plans for the Citrix XenApp system.
Vulnerability Discussion: Disaster recovery is the process of recognizing which threats have the potential to escalate into a disaster, and then taking steps to prevent or minimize the impact. This ensures mission critical systems can be restored quickly or within a short period of time after a disaster occurs. Disaster recovery plans concentrate on restoring data and technology and implementing systems that can prevent or minimize disasters. Disaster and recovery plans should be drafted and exercised in accordance with the MAC level of the system/Enclave as defined by the DoDI 8500.2. Disaster recovery plans provide for the resumption of mission or business essential functions. A disaster recovery plan must exist that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level. (Disaster recovery

procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance).

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0040 (Manual)

Request a copy of the disaster recovery plan from the IAO/SA. Review the plan to verify that the XenApp server and components are included in the plan. If the plan does not include the XenApp server or is incomplete this is a finding.

Fixes: CTX0040 (Manual)

Add the XenApp server to the disaster recovery plan.

Vulnerability Key: V0017993
STIG ID: CTX0050
Release Number: 1
Status: Active
Short Name: XenApp published applications are not approved.
Long Name: XenApp applications published to users are not approved by the IAO/SA.
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 Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0050
Severity: Category III
Long Name: XenApp applications published to users are not approved by the IAO/SA.
Vulnerability Discussion: XenApp makes information available to users by publishing resources on servers. The types of resources that may be published are applications installed on the XenApp server, the serverâ€™s desktop, and data files such as web pages, documents, media files, spreadsheets, and URLs. Resources published to users must be approved as sensitive data may inadvertently be published to unauthorized users.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: CTX0050 (Manual)

Request a copy of the documentation that lists all approved applications. If applications are

published to users that are not on the approved list, this is a finding. If no approved published applications list exists, this is a finding.

Fixes: CTX0050 (Manual)
Document and approve all XenApp published applications.

Vulnerability Key: V0017994
STIG ID: CTX0060
Release Number: 1
Status: Active
Short Name: XenApp is not in PNP database
Long Name: The Citrix XenApp server is not configured in the PNP database.
IA Controls: DCPP-1 Ports, Protocols, and Services
Categories: 14.2 Protocol Security
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0060
Severity: Category II
Long Name: The Citrix XenApp server is not configured in the PNP database.
Vulnerability Discussion: DoDI 8550.1 Ports, Protocols, and Services Management (PPSM) is the DoDâ€™s policy on IP Ports, Protocols, and Services (PPS). It controls the PPS that are permitted or approved to cross DoD network boundaries. Standard well known and registered IP ports and associated protocols and services are assessed for vulnerabilities and threats to the entire Global Information Grid (GIG) which includes the DISN backbone networks. The results are published in a Vulnerability Assessment (VA) report. Each port and protocol is given a rating of green, yellow, orange, or red in association with each of the 16 defined boundary types. Green means the protocol is relatively secure and is approved to cross the associated boundary without restrictions. Yellow means the protocol has security issues that must be mitigated to be used. Red means that the protocol is prohibited due to vulnerabilities that cannot be mitigated or approved, and is banned when crossing that boundary. The orange category requires DSAWG approval if the protocol exists and is necessary on the network. However, the orange category mandates that new systems and applications must not be developed using this protocol whether it crosses a boundary or not. The PPS Assurance Categories Assignment List (CAL) contains information regarding the assessed ports and protocols and defined boundaries, which is updated on a monthly basis. The PPSM information is available on the IASE and DKO/DoD IA Portal web sites. A portion of the DoDI 8550.1 PPS policy requires registration of those PPS that cross any of the boundaries defined by the policy that are â€œvisible to DoD-managed componentsâ€. Therefore, to comply with the policy and ensure that protocols and ports are acceptable, XenApp servers will be registered as automated information systems (AIS) with their associated TCP or UDP ports in the DoD Ports and Protocol

Registration System.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0060 (Manual)

If either inbound or outbound traffic to the XenApp server is leaving the local enclave, verify that the server has been registered in the Ports and Protocols (PNP) database (https://pnp.cert.smil.mil) for the site. If it is not registered this is a finding. If the traffic is completely contained within the local enclave, this requirement does not apply.

Fixes: CTX0060 (Manual)

Register all XenApp traffic that is leaving the local enclave in the PNP database for the site.

Vulnerability Key: V0017996
STIG ID: CTX0070
Release Number: 1
Status: Active
Short Name: There is no XenApp Configuration Control Board
Long Name: The Citrix XenApp server is not under the direct control of a configuration control board.
IA Controls: DCCB-1 Control Board
DCCB-2 Control Board
Categories: 12.4 CM Process
Effective Date: 29 Jun 2009

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

Condition: XenApp Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0070
Severity: Category II
Long Name: The Citrix XenApp server is not under the direct control of a configuration control board.
Vulnerability Discussion: Security integrity of the system and the ability to back-up and recover from failures cannot be maintained without the control of the system configuration. Unless the configuration is controlled by an independent board, it is much less likely to be in its approved accredited state. Testing and tracking any modifications to policies and procedures should be done thru a configuration control board. Security and integrity of the system and the ability to back-up and recover from failures cannot be maintained without the control of the system configuration. Unless the configuration is controlled by an independent board, it is much less likely to be in its approved accredited state.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: CTX0070 (Manual)

Ask to see the documented configuration management process for the XenApp server and/or farms. Ensure that the plan includes a site Configuration Control Board (CCB). If a plan that includes a CCB exists, this is not a finding. If a plan exists but does not include a CCB or there is not a plan, this is a finding.

Fixes: CTX0070 (Manual)

Implement a configuration management process for the XenApp server.

Vulnerability Key: V0019184
STIG ID: CTX0080
Release Number: 2
Status: Active
Short Name: XenApp Server audit logs are not reviewed.
Long Name: XenApp Server logs are not reviewed on a regular basis.
IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
Categories: 10.3 Review
Effective Date: 29 Jun 2009

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

Condition: XenApp Policy (Target: XenApp Policy)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: CTX0080
Severity: Category II
Long Name: XenApp Server logs are not reviewed on a regular basis.
Vulnerability Discussion: It is necessary to review XenApp Server, Web Interface Server, STA Server, and Secure Gateway Server logs or suspicious activity, problems, attacks, and system warnings will go undetected. These logs provide visibility into the activities and events of the servers. These logs enable system administrators and auditors the ability to recreate past events, monitor the system, and ensure security policies are being enforced.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
Checks: CTX0080 (Manual)

Ask the IAO/SA how often the logs are reviewed. Logs that should be reviewed daily include the Web Interface Server logs, the Secure Gateway Server logs, the STA logs, and XenApp Server logs. If the logs are not reviewed daily, this is a finding.

Fixes: CTX0080 (Manual)

Review all logs on a daily basis for the XenApp Farm.

Vulnerability Key: V0019185
STIG ID: CTX0120
Release Number: 1
Status: Active
Short Name: Authorized users of consoles are not reviewed.
Long Name: The authorized users of the Access Management and Presentation Server Consoles are not reviewed monthly.
IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting
Categories: 10.3 Review
Effective Date: 29 Jun 2009

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

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

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

STIG ID: CTX0120
Severity: Category II
Long Name: The authorized users of the Access Management and Presentation Server Consoles are not reviewed monthly.
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 opening up vulnerabilities and affecting the user community. It is essential to periodically review the authorized console users to ensure that no unauthorized users have been granted access to the consoles.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
Checks: CTX0120 (Manual)

Interview the IAO/SA and ask them how often the authorized users of the Access Management and Presentation Server consoles are reviewed. If it is not done on a monthly basis, this is a finding.

To check the authorized users, perform the following:
1.On the XenApp Server: Select Start > All Programs > Citrix > Management Consoles > Access Management Console
2. Select the <farm name> Administrators (The authorized users are listed here.)

Fixes: CTX0120 (Manual)

Review the Authorized users of the Access Management and Presentation Server consoles monthly.

Vulnerability Key: V0019199
STIG ID: CTX0110
Release Number: 1
Status: Active
Short Name: There is no policy on ICA client connections.
Long Name: There is no policy that instructs ICA clients to connect to only authorized and approved XenApp Servers.
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 Policy (Target: XenApp Policy)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: CTX0110
Severity: Category III
Long Name: There is no policy that instructs ICA clients to connect to only authorized and approved XenApp Servers.
Vulnerability Discussion: ICA Clients may connect to unauthorized or rogue XenApp Servers if configured incorrectly. Without guidance that documents which servers may be connected to for published applications, there is the possibility that users may reconfigure the ICA client to connect to other XenApp Servers. Therefore, there will be a policy in place that instructs users to use only approved and authorized XenApp Servers. These servers will be documented with the IAO.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation
Checks: CTX0110 (Manual)

Ask the IAO for the policy that instructs users to only connect to authorized and approved XenApp Servers. These servers must be listed in the document. If no document or policy is available, this is a finding.

Fixes: CTX0110 (Manual)

Create a policy that instructs users to only connect to authorized and approved XenApp Servers.

Vulnerability Count - 10