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 Secure Gateway Server

---

**Vulnerability Key:** V0018219
**STIG ID:** CTX0700
**Release Number:** 2
**Status:** Active
**Short Name:** Secure Gateway Servers are not located in the DMZ.
**Long Name:** Secure Gateway Servers are not located in the DMZ or screened subnet.
**IA Controls:** ECSC-1 Security Configuration Compliance
**Categories:** 4.4 DMZ
**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

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

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

**STIG ID:** CTX0700
**Severity:** Category II
**Long Name:** Secure Gateway Servers are not located in the DMZ or screened subnet.

**Vulnerability Discussion:** 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 the Internet to the enterprise network. The Secure Gateway allows the tunneling of all ICA client traffic using SSL/TLS. The Secure Gateway manages the connectivity and encryption across the public Internet and hides the XenApp farm from potential intruders.

**Responsibility:** System Administrator
Information Assurance Officer

**References:** Department of Defense Instruction 8500.2 (DODI 8500.2)

**Checks:**

CTX0700 (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 Secure Gateway servers. Access the Secure Gateway server and type the following at the command prompt:

C:\>ipconfig /all

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

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

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

**Fixes:**

CTX0700 (Manual)

Place the Secure Gateway Server in the DMZ or screened subnet.

---

**Vulnerability Key:** V0018220
**STIG ID:** CTX0710
**Release Number:** 1
**Status:** Active
**Short Name:** Secure Gateway certs are not DoD approved certs
**Long Name:** Secure Gateway certificates are not DoD approved certificates.
**IA Controls:** DCNR-1 Non-repudiation
**Categories:** 1.2 PKI
**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0710

**Severity:** Category II

**Long Name:** Secure Gateway certificates are not DoD approved certificates.

**Vulnerability Discussion:** User sessions with Citrix Secure Gateway 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 Secure Gateway 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:**

CTX0710 (Manual)

1. Access the Secure Gateway Server and review the certificates in the following location:
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:**

CTX0710 (Manual)

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

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

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

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

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

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

2. Navigate to the OpenSSL directory (c:\openssl\bin\) on the 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 â€œUSâ€
For State or Province Name, type â€œ.â€
For Locality Name, type â€œ.â€
For Organization Name, type â€œU.S. Governmentâ€
For Organizational Unit Name, type â€œOU=DISA, OU=PKI, OU=DoDâ€
For Common Name, type your Fully Qualified Domain Name of your server (i.e.server.disa.mil)
For Email Address, type your email address

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

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

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

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

---

**Vulnerability Key:** V0018221
**STIG ID:** CTX0720
**Release Number:** 2
**Status:** Active
**Short Name:** Secure Gateway Server secure protocol set to COM.
**Long Name:** Secure Gateway Server secure protocol is set to COM.
**IA Controls:** DCNR-1 Non-repudiation
**Categories:** 1.2 PKI
**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)
**Policy:** All Policies
**MAC /**

**Confidentiality Grid:**

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

**STIG ID:** CTX0720

**Severity:** Category II

**Long Name:** Secure Gateway Server secure protocol is set to COM.

**Vulnerability Discussion:** User sessions with Citrix Secure Gateway 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 Secure Gateway will be encrypted with a Federal Information Processing Standard (FIPS) 140-2 encryption algorithm. The US government requires the use of TLS to secure data communications. FIPS 140 is a standard for cryptography. The XenApp COM cipher suites are: SSL_RSA_WITH_RC4_128_MD5 and SSL_RSA_WITH_RC4_128_SHA. The GOV cipher suite is: SSL_RSA_WITH_3DES_EDE_CBC_SHA. The XenApp GOV cipher suite meets the required FIPS requirements.

**Responsibility:** System Administrator
Information Assurance Officer

**References:** Department of Defense Instruction 8500.2 (DODI 8500.2)

**Checks:** CTX0720 (Manual)

Access the Secure Gateway Server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console.
2. Open the Secure Gateway Configuration.
3. Select Advanced.
4. Click through the wizard and verify that Transport Layer Security (TLSv1) and GOV cipher suite is selected. If these are not selected, this is a finding.

**Fixes:** CTX0720 (Manual)

Configure the secure protocols to TLS and GOV.

---

**Vulnerability Key:** V0018222

**STIG ID:** CTX0730

**Release Number:** 1

**Status:** Active

**Short Name:** STA server traffic is not encrypted.

**Long Name:** Secure Gateway server to Secure Ticket Authority (STA) server traffic is not encrypted.

**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<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0730

**Severity:** Category II

**Long Name:** Secure Gateway server to Secure Ticket Authority (STA) server traffic is not encrypted.

**Vulnerability Discussion:** The Secure Gateway may be configured as a gateway between SSL/TLS-enabled clients and servers. The enclave traffic between XenApp servers and the Secure Gateway server is encrypted using SSL/TLS. This ensures that XenApp servers are able publish information remotely without compromising security. The Secure Gateway transparently encrypts and authenticates all connections to protect against eavesdropping and data tampering. Without this encryption, traffic between the XenApp server and the Secure Gateway is sent in plaintext.

**Responsibility:** System Administrator
Information Assurance Officer

**References:** Department of Defense Instruction 8500.2 (DODI 8500.2)

**Checks:** CTX0730 (Manual)

Access the Secure Gateway server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console.
2. Open the Secure Gateway Configuration.
3. Select Advanced.
4. Click through the wizard until you get to the â€œDetails of the server running the Secure Ticket Authority (STA)â€. Click on Modify in the â€œServers running the STA:â€ box.
5. Verify that the â€œProtocol Settings:â€ box has the â€œSecure traffic between the STA and the Secure Gatewayâ€ checked. If not, this is a finding.

**Fixes:** CTX0730 (Manual)

Encrypt all traffic between the secure gateway and the XenApp STA server.

---

**Vulnerability Key:** V0018225

**STIG ID:** CTX0740

**Release Number:** 1

**Status:** Active

**Short Name:** Web Interface traffic is not encrypted.

**Long Name:** Secure Gateway to Web Interface traffic is not encrypted.

**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<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0740

**Severity:** Category II

**Long Name:** Secure Gateway to Web Interface traffic is not encrypted.

**Vulnerability Discussion:** The Secure Gateway may be configured as a gateway between SSL/TLS-enabled clients and servers. The Web Interface traffic between the Secure Gateway server is encrypted using SSL/TLS. This ensures that Web Interface servers are able to publish information remotely without compromising security. The Secure Gateway transparently encrypts and authenticates all connections to protect against eavesdropping and data tampering. Without this encryption, traffic between the Web Interface server and the Secure Gateway is sent in plaintext. Plaintext 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:** CTX0740 (Manual)

If the Web Interface is installed on the same server, this check is not applicable. To determine if the Web Interface is installed on the same then server perform the following:
1. Select Start > Control Panel > Add or Remove Programs.
2. If Citrix Web Interface is installed, then open the Access Management Console and verify that there is a website created for publishing applications.

If the Web Interface is not installed on the same server, perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console.
2. Open the Secure Gateway Configuration.
3. Select Advanced.
4. Click through the wizard until you get to the â€œDetails of the server running the Web Interfaceâ€. Verify that the â€œSecure traffic between the Web Interface and the Secure Gatewayâ€ is checked. If not, this is a finding.

**Fixes:** CTX0740 (Manual)

Encrypt traffic between the Web Interface server and Secure Gateway server.

---

**Vulnerability Key:** V0018226

**STIG ID:** CTX0750

**Release Number:** 1

**Status:** Active

**Short Name:** Concurrent connection limits are unlimited.

**Long Name:** Secure Gateway concurrent connection limits are configured to unlimited.

**IA Controls:** ECLO-1 Logon

**Categories:** 12.4 CM Process

**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open | Comments: |

| | |
|---|---|
| ☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0750

**Severity:** Category II

**Long Name:** Secure Gateway concurrent connection limits are configured to unlimited.

**Vulnerability Discussion:** By configuring the concurrent connection to unlimited, this may create a denial of service to users trying to access the Secure Gateway server. To ensure XenApp applications do not consume or cripple the Secure Gateway server, specify the maximum number of concurrent connections for the server. The default concurrent connection limit is 250.

**Responsibility:** System Administrator
Information Assurance Officer

**References:** Department of Defense Instruction 8500.2 (DODI 8500.2)

**Checks:** CTX0750 (Manual)

Access the Secure Gateway server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console.
2. Open the Secure Gateway Configuration.
3. Select Advanced.
4. Click through the wizard until you get to the â€œConnection Parametersâ€. Verify that the â€œUnlimitedâ€ checkbox is not checked in the â€œConcurrent connection limitsâ€. If it is, this is a finding. The default "Concurrent connection limits" is 250.

**Fixes:** CTX0750 (Manual)

Do not configure concurrent connection limits to unlimited.

---

**Vulnerability Key:** V0018231

**STIG ID:** CTX0760

**Release Number:** 1

**Status:** Active

**Short Name:** No connection timeout limit is configured.

**Long Name:** Secure Gateway is not configured with a connection timeout limit.

**IA Controls:** ECLO-1 Logon
ECLO-2 Logon

**Categories:** 12.4 CM Process

**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable | Comments: |

| | |
|---|---|
| ☐ Not Reviewed | |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0760

**Severity:** Category II

**Long Name:** Secure Gateway is not configured with a connection timeout limit.

**Vulnerability Discussion:** The connection timeout limit is set in minutes. If the connection timeout is configured to unlimited, then chances increase that a user may get distracted and walk away from the client device, potentially leaving the session accessible to unauthorized users.

**Responsibility:** System Administrator
Information Assurance Officer

**References:** Department of Defense Instruction 8500.2 (DODI 8500.2)

**Checks:**

CTX0760 (Manual)

Access the Secure Gateway server and perform the following:
1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console.
2. Open the Secure Gateway Configuration.
3. Select Advanced.
4. Click through the wizard until you get to the â€œConnection Parametersâ€. Verify that the â€œNo connection timeoutâ€ box is not checked. If it is checked, this is a finding.

**Fixes:**

CTX0760 (Manual)

Configure connection timeouts for all Secure Gateway server sessions.

---

**Vulnerability Key:** V0018232
**STIG ID:** CTX0770
**Release Number:** 2
**Status:** Active
**Short Name:** Secure Gateway Server has incorrect VMS posture.
**Long Name:** The Secure Gateway 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<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0770

**Severity:** Category II

**Long Name:** The Secure Gateway 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:**

CTX0770 (Manual)

1. If VMS is not used, this check is not applicable.
2. If the assets are registered in VMS, verify that the following postures are registered.

Win2k3
AntiVirus
XenApp Secure Gateway Server

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

**Fixes:**

CTX0770 (Manual)

Configure all Secure Gateway assets into VMS with the correct posture.

---

**Vulnerability Key:** V0019181

**STIG ID:** CTX0780

**Release Number:** 1

**Status:** Active

**Short Name:** Inbound connections are not restricted.

**Long Name:** Inbound connections to the Secure Gateway Server are not restricted to specific IP Interfaces.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

| | | | |
|---|---|---|---|
| **Public** | ☑ | ☑ | ☑ |

**STIG ID:** CTX0780

**Severity:** Category III

**Long Name:** Inbound connections to the Secure Gateway Server are not restricted to specific IP Interfaces.

**Vulnerability Discussion:** The default behavior of the Citrix Secure Gateway is to monitor all IP addresses (thereby all network cards with an IP stack bound to them) for incoming connections. If the server has multiple network cards, the Secure Gateway could receive requests on any IP under the default configuration. If the server performs roles other than Secure Gatway or has multiple network cards, then traffic will be received on all cards. Configuring only the required network cards for Secure Gateway traffic limits the inbound traffic that it will listen on. This provides more granular control and a smaller attack surface for outside connections.

**Responsibility:** System Administrator
Information Assurance Officer

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

**Checks:** CTX0780 (Manual)

Access the Secure Gateway server and perform the following: 1. Select Start > All Programs > Citrix > Management Consoles > Secure Gateway Management Console. 2. Open the Secure Gateway Configuration. 3. Select Advanced. 4. Click through the wizard until you get to the â€œConfigure inbound client connections".
5. Verify that the â€œNetwork Interface list" is only configured to listen only on specified IP addresses and ports. If the "Monitor all IP addresses" box is selected, this is a finding

**Fixes:** CTX0780 (Manual)

Configure the Secure Gateway inbound client connections to specific IP addresses and ports.

---

**Vulnerability Key:** V0019182

**STIG ID:** CTX0790

**Release Number:** 1

**Status:** Active

**Short Name:** Unauthorized users have access to SG logs.

**Long Name:** Unauthorized users have more than read access to the Secure Gateway logs.

**IA Controls:** ECTP-1 Audit Trail Protection

**Categories:** 2.1 Object Permissions

**Effective Date:** 29 Jun 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0790

**Severity:** Category II

**Long Name:** Unauthorized users have more than read access to the Secure Gateway logs.

**Vulnerability Discussion:** It is critical to protect system Secure Gateway log files from being modified or accessed by unauthorized individuals. Some logs may contain sensitive data that should only be available to the auditors group.

**Responsibility:** System Administrator
Information Assurance Officer

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

**Checks:** CTX0790 (Manual)

Access the Secure Gateway server and perform the following:
1. Open Windows Explorer and navigate to the following path:The default path for the error logs is the installation path for the Secure Gateway typically %systemroot%\Program Files\Citrix\Secure Gateway\logs.
2. Right click on the logs folder, select the security tab, and verify only the following groups have greater than READ access:
Auditors (Could be Active Directory Domain group or Local Machine Group)
SYSTEM
NETWORK SERVICE

If other users are listed and have greater than READ access, this is a finding. (ie, administrators with modify, full control, etc.)

**Fixes:** CTX0790 (Manual)

Ensure that only the Auditors, Network Service and System groups have full access to the Secure Gateway logs. All other groups will only have read access.

---

**Vulnerability Key:** V0021554
**STIG ID:** CTX0765
**Release Number:** 1
**Status:** Active
**Short Name:** Secure Gateway Server is not registered in VMS.
**Long Name:** The Secure Gateway Server is not registered in VMS or vulnerability database system.
**IA Controls:** VIVM-1 Vulnerability Management
**Categories:** 12.5 IAVM Process
**Effective Date:** 14 Oct 2009

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

**STIG ID:** CTX0765

**Severity:** Category II

**Long Name:** The Secure Gateway Server is not registered in VMS or vulnerability database system.

**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 Secure Gateway Server 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:** CTX0765 (Manual)

If VMS is used, then ensure the Secure Gateway 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:** CTX0765 (Manual)

Register Secure Gateway Servers in VMS or vulnerability management database.

---

**Vulnerability Key:** V0026086
**STIG ID:** 2011-B-0028
**Release Number:** 1
**Status:** Active
**Short Name:** 2011-B-0028
**Long Name:** Citrix Secure Gateway Remote Code Execution Vulnerability
**IA Controls:** ECMT-1 Conformance Monitoring and Testing
ECMT-2 Conformance Monitoring and Testing
VIVM-1 Vulnerability Management
**Categories:** 12.5 IAVM Process
**Effective Date:** 03 Mar 2011

| | |
|---|---|
| ☐ Open<br>☐ Not a Finding<br>☐ Not Applicable<br>☐ Not Reviewed | Comments: |

**Condition:** XenApp Secure Gateway Server (Target: XenApp Secure Gateway Server)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

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

| | | | |
|---|---|---|---|
| **Public** | ☑ | ☑ | ☑ |

**STIG ID:** 2011-B-0028

**Severity:** Category II

**Long Name:** Citrix Secure Gateway Remote Code Execution Vulnerability

**Vulnerability Discussion:** Citrix has released a security advisory addressing a vulnerability in Citrix Secure Gateway. Citrix Secure Gateway is a Citrix Access Suite infrastructure component used to securely access Citrix Presentation Server farms. To exploit this vulnerability, a remote attacker would use various tactics, techniques and procedures to exploit this vulnerability. If successfully exploited, this vulnerability would allow an attacker to execute arbitrary code and compromise the affected system. At this time, there are no known exploits associated with this vulnerability; USCYBERCOM is not aware of any DoD related incidents. Remote Code Execution Vulnerability in Citrix Secure Gateway: A vulnerability has been identified in Citrix Secure Gateway that, when triggered, could result in arbitrary code being executed on the server in the context of the Secure Gateway process. This vulnerability only affects Secure Gateway version 3.1.4. Secure Gateway version 3.2.0 is not affected by this vulnerability, but Citrix recommends that customers currently using this version upgrade their deployments to version 3.2.1 in line with the guidance provided in CTX123359.

**Responsibility:** System Administrator

**References:** Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, â€œDefense-in-Depth: Information Assuran Citrix Security Advisory (Created within IAVA process)
Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, â€œDefense-in-Depth: Information Assuran IAVM DMS Message (Created within IAVA process)
Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, â€œDefense-in-Depth: Information Assuran Secunia (Created within IAVA process)
Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, â€œDefense-in-Depth: Information Assuran Symantec Deepsight BID 46596 (requires account) (Created within IAVA process)

**Checks:**

**Fixes:** Upgrade to non-vulnerable Citrix Product (IAVA)

Fix Action: Upgrade to non-vulnerable version of affected Citrix product

Note: System administrators should refer to the Citrix Security Advisory to determine affected applications/system and appropriate fix actions.

---

## Vulnerability Count - 12