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: Sun Ray 4

Vulnerability Key:	V0016061
STIG ID:	SUN0020
Release Number:	4
Status:	Active
Short Name:	Sun Ray Desktop Unit traffic is not isolated
Long Name:	Sun Ray Desktop Unit traffic is not isolated logically through the use of a dedicated VLAN or network segment.
IA Controls:	ECSC-1 Security Configuration Compliance
Categories:	12.4 CM Process
Effective Date:	12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0020

Severity: Category II

Long Name: Sun Ray Desktop Unit traffic is not isolated logically through the use of a dedicated VLAN or network segment.

Vulnerability Discussion: Isolated LANs provide a greater degree of security than traditional LANs since only authorized users and devices are allowed to connect. Authorized users and devices are configured through the use of access control lists. This logical separation provides better performance through broadcast reduction, and reduced configuration management for Sun Ray Desktop Unit device moves, additions, and changes.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0020 (Manual)

Work with the network reviewer and system administrator to determine compliance. Request a copy of switch configuration to verify the ports that the Sun Ray server plugs into are configured to a dedicated VLAN. Below is an example of a VLAN that may be used for Sun Ray server traffic.

Cisco IOS Example:

```
Interface VLAN5
description “Network A”
ip address 192.168.1.25 255.255.255.0
no shutdown

interface VLAN 12
description “Network Sun Ray”
ip address 10.0.0.25 255.255.255.0
no shutdown

set interface sc0 10.0.0.25 255.255.255.0
```

Fixes:

SUN0020 (Manual)

Isolate Sun Ray Desktop Unit traffic from other traffic.

Vulnerability Key: V0016062
STIG ID: SUN0030
Release Number: 5
Status: Active
Short Name: Users are not forced to authenticate to SRSS.
Long Name: Users are not forced to authenticate to the Sun Ray Server.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 12.4 CM Process
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality

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

Grid:

	☑	☑	☑
Sensitive	☑	☑	☑
Public	☑	☑	☑

STIG ID: SUN0030
Severity: Category II
Long Name: Users are not forced to authenticate to the Sun Ray Server.
Vulnerability Discussion: Two-factor authentication identifies users using two distinctive factors--something they have and something they know or something they are. Requiring two different forms of electronic identification reduces the risk of fraud. The DoD employs the use of a Common Access Card for the NIPRnet. CAC cards are microprocessor cards that offer security independent of the reader device, making it ideal for high-security applications. With microprocessor cards, a user's private key is securely stored within the smart card and never leaves the card. Using the onboard processor, all cryptographic functions, including digital signatures and decryption of session keys, occur inside the card. For SIPRnet, Common Access Cards are not currently being used for authentication and identification on the SIPRNet. The Sun Ray systems will have this feature disabled until such a time when the SIPRNet PKI infrastructure is in place to support this functionality. Disabling this feature will ensure that users don't place NIPRNet Common Access Card certificates on the SIPRNet.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

SUN0030 - NIPRNET (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the System Policy Tab.
3. Verify the Card Users Access has "Users with Registered Tokens" selected.
4. If Access is set to "None", or "All Users", this is a finding.

SUN0030-SIPRNET (Manual)

Within the Sun Ray Administration console, perform the following: 1. Select the Advanced Tab. 2. Select the System Policy Tab. 3. Verify the Non-Card Users Access has "Users with Registered Tokens" selected. 4. If Access is set to "None" or "All Users", this is a finding.

Fixes:

SUN0030 (Manual)

Authenticate users to the SRSS Server based on the classification of the system.
NIPRNET - Within the Sun Ray Administration console, perform the following: 1. Select the Advanced Tab. 2. Select the System Policy Tab. 3. Check the Card Users Access for "Users with Registered Tokens".
SIPRNET - Within the Sun Ray Administration console, perform the following: 1. Select the Advanced Tab. 2. Select the System Policy Tab. 3. Check the Non-Card Users Access for "Users with Registered Tokens".

Vulnerability Key: V0016063
STIG ID: SUN0040
Release Number: 6
Status: Active
Short Name: Users kiosk mode timeout has no value.
Long Name: Users kiosk mode timeout is configured with no value.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 12 Sep 2008

☐ Open ☐ Not a Finding	Comments:

☐ Not Applicable ☐ Not Reviewed	

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0040

Severity: Category III

Long Name: Users kiosk mode timeout is configured with no value.

Vulnerability Discussion: If no value is specified for the number of seconds for a disconnected kiosk session, the termination of disconnected sessions will be disabled. This could potentially leave open sessions and may cause the kiosk sessions to start incorrectly or to crash due to lack of resources from many sessions being open.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0040 (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the Kiosk Mode Tab.
3. Click on the Edit button.
4. Select the preferred Kiosk Session from the Session drop-down list and verify the Timeout box has a value of 10 minutes or less, but not zero. The default is 12000 seconds. If it is greater than 600 seconds (10 minutues) or zero/blank, this is a finding. Should be configured to 600 seconds or less.

Fixes:

SUN0040 (Manual)

Configure the Sun Ray Kiosk mode timeout value with a value of 10 minutes or less.

Vulnerability Key: V0016064
STIG ID: SUN0050
Release Number: 6
Status: Active
Short Name: Self-registration is permitted for users.
Long Name: Self-registration is permitted for users.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0050

Severity: Category I

Long Name: Self-registration is permitted for users.

Vulnerability Discussion: Sun Ray Desktop Unit users are not registered centrally for users by the system administrator. With self-registration, the system administrator does not assign registered tokens to the authorized users. This poses a security risk since users may be able to register themselves in the Sun Ray administration database. If an unauthorized user obtains access to a Sun Ray Desktop unit, then that user may be able to start a session without any intervention from the system administrator.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0050-SIPRNET (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the System Policy Tab.
3. Verify the Non-Card Users Access has “Self Registration Allowed” not checked.
4. If Access is set to "Self-Registration Allowed", this is a finding.

SUN0050-NIPRNET (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the System Policy Tab.
3. Verify the Card Users Access has “Self Registration Allowed” not checked.
4. If Access is set to "Self-Registration Allowed", this is a finding.

Fixes:

SUN0050 (Manual)

Disable Self-Registration for all users.
NIPRNET - Within the Sun Ray Administration console, perform the following: 1. Select the Advanced Tab. 2. Select the System Policy Tab. 3. Uncheck the Card Users Access for “Self Registration Allowed”.
SIPRNET - Within the Sun Ray Administration console, perform the following: 1. Select the Advanced Tab. 2. Select the System Policy Tab. 3. Uncheck the Non-Card Users Access for “Self Registration Allowed”.

Vulnerability Key: V0016071

STIG ID: SUN0070

Release Number: 5

Status: Active

Short Name: Default administrator account is used.

Long Name: Default administrator account is used to access the administration tool.

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

Categories: 2.2 Least Privilege

Effective Date: 15 Sep 2008

Open	Comments:

☐ ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0070

Severity: Category I

Long Name: Default administrator account is used to access the administration tool.

Vulnerability Discussion: The default administrator account, “admin”, does not provide an audit trail of who logged in and the default password may be easily guessed or be publicly known. If system administrators use the “admin” account, this could potentially allow modifications to the Sun Ray system with no user accountability. Also, unauthorized users may gain access to the administration tool and make modifications that disable the Sun Ray system. Therefore, system administrators will have individual user accounts to administer the Sun Ray Server, and the “admin” account will be removed to ensure that audit trails are present.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0070 (Manual)

1. Open a terminal command line on the Sun Ray server. Perform the following:
/opt/SUNWut/sbin/utadminuser
admin

If the admin user is returned, this is a finding.

2. Then verify that the following /etc/pam.conf file has the following entries:
Use the following command to locate them.
cat /etc/pam.conf | grep utadmingui

added to utadmingui by Sun Ray Server Software -- utadmingui
utadmingui auth requisite pam_authtok_get.so.1
utadmingui auth required pam_dhkeys.so.1
utadmingui auth required pam_unix_cred.so.1
utadmingui auth required pam_unix_auth.so.1

If the above entries are not in the /etc/pam.conf file, then the alternate username specified to administer the Sun Ray administration tool will not work.

If above entries are not in the pam.conf file, this is a finding.

Fixes:

SUN0070 (Manual)

Configure individual usernames to access the Sun Ray administration console.

Vulnerability Key: V0016072
STIG ID: SUN0080

Release Number: 3
Status: Active
Short Name: Unauthorized users have access to admin tool
Long Name: Unauthorized users have access to the Sun Ray administration tool.
IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.2 Least Privilege
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0080
Severity: Category I
Long Name: Unauthorized users have access to the Sun Ray administration tool.
Vulnerability Discussion: Unauthorized users accessing the Sun Ray administration tool could modify or disable the entire Sun Ray server or network. Unrestricted access may also give access to other operating system daemons and applications. Restricting the Sun Ray administrator tool to only authorized users will ensure that only authorized users will have access to the Sun Ray configuration.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0080 (Manual)

Request the documentation authorizing users to administer the Sun Ray Server. Compare this list with the list below. If there is a discrepancy, this is a finding.
Open a terminal command line on the Solaris 10 server. Perform the following:
/opt/SUNWut/sbin/utadminuser

If users listed here are not authorized to access the Sun Ray administration console, this is a finding.

Fixes: SUN0080 (Manual)

Ensure only authorized users have access to the Sun Ray administration console.

Vulnerability Key: V0016075
STIG ID: SUN0090
Release Number: 2
Status: Active
Short Name: Sun Ray Server admin session default timeout used
Long Name: Sun Ray Server administrator session default timeout is used.

IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0090
Severity: Category II
Long Name: Sun Ray Server administrator session default timeout is used.
Vulnerability Discussion: Administrator sessions to the Sun Ray Server are critical to the availability and integrity of the system. The default timeout for these sessions is 30 minutes of inactivity. This session timeout is longer than the 10 minutes required by the Operating System and Network STIGs. Therefore, all administrator sessions will be configured to 10 minutes of inactivity to ensure unauthorized users do not gain access to the system configuration.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

SUN0090 (Manual)

On the Sun Ray server perform the following:
cat /etc/opt/SUNWut/webamin/webadmin.conf | grep session.timeout

# The session timeout (specified in minutes)
Session.timeout=10

If the “session.timeout” value does not equal 10 minutes or less, this is a finding.

Fixes:

SUN0090 (Manual)

Configure the administrator session timeout value to 10 minutes or less.

Vulnerability Key: V0016083
STIG ID: SUN0110
Release Number: 2
Status: Active
Short Name: Sun Ray DTUs firmware not at minimum version
Long Name: Sun Ray Desktop Units firmware is not at the minimum version.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 3.1 Security Patches
3.2 Operational / PM Patches

Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0110

Severity: Category II

Long Name: Sun Ray Desktop Units firmware is not at the minimum version.

Vulnerability Discussion: All Sun Ray firmware is supported by the Sun Ray Desktop Units PROM. Therefore, older versions of the Sun Ray firmware may not be as secure as newer versions. In order to support encryption between the Sun Ray Desktop Unit and the Sun Ray server, the minimum firmware required is version 2.0. All previous Sun Ray Desktop Unit firmware sends traffic in plain text to the server

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0110 (Manual)

The server may have newer patch version of the firmware installed, but the clients may not have downloaded the new firmware due to policy restrictions. Therefore, it is important to check the firmware on the client, not the server. To check the firmware, go to the Sun Ray Desktop Unit, and perform the following:

On the Sun Ray 2fs unit press the (Stop-V) on Sun Keyboard and on the PC keyboards press the (Ctrl-Pause-V).
If the version is lower than 2.0, this is a finding. Most likely the version will be 4.0.-127553-02.2008-03.06.15.04 or higher.

Note: For other Sun Ray Desktop Units, consult the system administrator or documentation for the key mode combinations.

Fixes:

SUN0110 (Manual)

Upgrade the firmware to 2.0 or higher, preferably to the most current firmware released from Sun Microsystems.

Vulnerability Key: V0016100

STIG ID: SUN0120

Release Number: 4

Status: Active

Short Name: Sun Ray Server software patches not tested

Long Name: Sun Ray Server software patches are not tested in a development environment first before deploying to production.

IA Controls: DCCT-1 Compliance Testing

Categories: 3.1 Security Patches

3.2 Operational / PM Patches

Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0120

Severity: Category II

Long Name: Sun Ray Server software patches are not tested in a development environment first before deploying to production.

Vulnerability Discussion: Organizations need to stay current with all applicable Sun Ray Server software updates that are released from Sun Microsystems. New Sun Ray Server patches and updates should be reviewed for the Sun Ray Server before moving them into a production environment. Sun Ray Server patches will be tested first in a development environment and any issues or special precautions will be documented, as a patch could technically disable all Sun Ray Desktop Units, cause unexpected performance or availability issues.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0120 (Manual)

1. Ask the IAO/SA where the test and development Sun Ray Servers are located. Access those servers and perform the following commands:

/opt/SUNWut/lib/utspatches

Should return the following:
127554-02
127557-01
OR
patchadd –p | grep <patch>

SRSS Patches need to be at one of the following:
Solaris/SPARC 127553
Solaris/x86 127554
Linux/x86 127555

SRWC 2.0 Patches need to be at one of the following:
Solaris/SPARC 127556
Solaris/x86 127557
Linux/x86 127558

If the preceding patches are not returned, this is a finding. Check Sun Microsystems's website for updated patches that may have been released after this checklist.

2. Request from the IAO/SA for a documented procedure on how their patches are tested on a development system before using on production systems. If no procedure is provided, this is a finding.

Fixes: SUN0120 (Manual)

Implement the latest patches for the Sun Ray system. Check Sun Microsystems's website for updated patches that may have been released after this checklist. Create patch procedures for testing before deploying patches to the production system.

Vulnerability Key: V0016103
STIG ID: SUN0130
Release Number: 3
Status: Active
Short Name: Sun Ray Server not current with latest patches
Long Name: The Sun Ray server software is not current with the latest available patches.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 3.1 Security Patches
3.2 Operational / PM Patches
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0130
Severity: Category II
Long Name: The Sun Ray server software is not current with the latest available patches.
Vulnerability Discussion: Sun Ray software patches mitigate many known vulnerabilities. To ensure that attackers cannot take advantage of known Sun Ray vulnerabilities, applicable software patches must be applied as they are released.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0130 (Manual)

On the Sun Ray server perform the following:

/opt/SUNWut/lib/utspatches

Should return the following:
127554-02
127557-01

OR

patchadd –p | grep <patch>

SRSS Patches need to be at one of the following:
Solaris/SPARC 127553
Solaris/x86 127554
Linux/x86 127555

SRWC 2.0 Patches need to be at one of the following:
Solaris/SPARC 127556
Solaris/x86 127557
Linux/x86 127558

If the preceding patches are not returned, this is a finding. Check Sun Microsystems's website for updated patches that may have been released after this checklist.

Fixes: SUN0130 (Manual)
Implement the latest patches for the Sun Ray system. Check Sun Microsystem's website for updated patches that may have been released after this checklist.

Vulnerability Key: V0016143
STIG ID: SUN0140
Release Number: 4
Status: Active
Short Name: USB ports not disabled for all Sun Ray DTU
Long Name: USB ports are not disabled for all Sun Ray Desktop Units. This requirement excludes the keyboard and mouse.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0140
Severity: Category II
Long Name: USB ports are not disabled for all Sun Ray Desktop Units. This requirement excludes the keyboard and mouse.
Vulnerability Discussion: Enabled USB ports may be used by users to store files, scripts, and executables. USB thumb drives, USB hard drives, and USB appliances may be inserted into these ports. If unapproved executables, scripts, or malware reside on the USB device, executing these or moving these onto the network may cause a virus infection or unapproved applications running on the network.

Classified data may be copied inadvertently to the unclassified network if ports have been enabled. Limiting the use of these ports will prevent these USB programs and files from accessing the network.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0140 (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the Security Tab.
3. Verify the USB Port under Devices is not checked. If it is, this is a finding.

Caveat: This is not applicable for keyboard and mouse USB ports, however, these ports must be documented and approved by the IAO. This check may be Not a Finding for USB ports enabled for operational purposes that are approved by the DAA.

Fixes:

SUN0140 (Manual)

Disable all USB ports on Sun Ray Desktop Units.

Vulnerability Key: V0016145
STIG ID: SUN0160
Release Number: 2
Status: Active
Short Name: Sun Ray server console admin session not encrypted
Long Name: The Sun Ray server console administration sessions are 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: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0160
Severity: Category II
Long Name: The Sun Ray server console administration sessions are not encrypted.
Vulnerability Discussion: Unencrypted Sun Ray server console sessions do not protect the information transmitted from being read or viewed by anyone. Unencrypted sessions are vulnerable to a number of attacks to include man-in-the-middle attacks, TCP Hijacking, and replay.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0160 (Manual)

Have the administrator log into the Sun Ray administrator console by typing the following: http://localhost:1660. If the session does not switch to https://localhost:1661 in the browser, this is a finding.

Fixes: SUN0160 (Manual)

Encrypt all Sun Ray server console sessions.

Vulnerability Key: V0016146
STIG ID: SUN0170
Release Number: 3
Status: Active
Short Name: Sun Ray DTU to server communication not encrypted
Long Name: Sun Ray Desktop Unit to server communication is not encrypted.
IA Controls: DCSR-1 Specified Robustness - Basic
DCSR-2 Specified Robustness - Medium
DCSR-3 Specified Robustness - High
Categories: 8.1 Encrypted Data in Transit
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0170
Severity: Category II
Long Name: Sun Ray Desktop Unit to server communication is not encrypted.
Vulnerability Discussion: In earlier versions of Sun Ray Server Software, data packets on the Sun Ray interconnect were sent in the clear or in plaintext. This made it easy to “snoop” the traffic and recover vital and private user information, which malicious users might misuse. To avoid this type of attack, Sun Ray Server Software allows administrators to enable traffic encryption. The encryption algorithm used is the ARCFOUR or RC4. NOTE: Terminal Services for Windows 2000 uses the same RC4 encryption algorithm. RDP traffic is encrypted using 128 bit encryption. The algorithm used for encryption depends on the encryption mode. Windows 2003 is FIPS compliant. In FIPS mode, 3DES and SHA1 are used. In non-FIPS mode, RC4 (encryption) and MD5 (keyed hashing) are used.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0170 (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.

2. Select the Security Tab.
3. Verify that “Upstream Encryption” and “Downstream Encryption” are checked.
4. If these are not checked, this is a finding.

Fixes: SUN0170 (Manual)

Encrypt Sun Ray traffic to all Desktop Units.

Vulnerability Key: V0016148
STIG ID: SUN0180
Release Number: 2
Status: Active
Short Name: Server Authentication is not configured
Long Name: Server Authentication is not configured on the Sun Ray server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0180
Severity: Category II
Long Name: Server Authentication is not configured on the Sun Ray server.
Vulnerability Discussion: It is possible to spoof a Sun Ray server or a Sun Ray client and pose as either. This leads to the man-in-the-middle attack, in which an impostor claims to be the Sun Ray server for the clients and pretends to be a client for the server. It then goes about intercepting all the messages and having access to all the secure data. Client and server authentication can resolve this type of attack. Server-side authentication is only supported, through the pre-configured public-private key pairs in Sun Ray Server Software and firmware. The Digital Signature Algorithm (DSA) is used to verify that clients are communicating with a valid Sun Ray server. This authentication scheme is not completely foolproof, but it mitigates man-in-the-middle attacks and makes it harder for attackers to spoof Sun Ray Server Software.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0180 (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the Security Tab.
3. Verify that “Server Authentication” is checked. If it is not checked, this is a finding.

Fixes:

SUN0180 (Manual)
Enable Server Authentication for the Sun Ray server.

Vulnerability Key: V0016151
STIG ID: SUN0190
Release Number: 2
Status: Active
Short Name: Security Mode is not configured to "Hard"
Long Name: The Security Mode is not configured to “Hard” on the Sun Ray server.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0190
Severity: Category I
Long Name: The Security Mode is not configured to “Hard” on the Sun Ray server.
Vulnerability Discussion: Soft security mode ensures that every client requesting a session gets one, even if security requirements cannot be met. As a result, the soft security mode grants insecure sessions. Hard security mode ensures that every session is secure. If security requirements cannot be met, the session is refused.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0190 (Manual)

Within the Sun Ray Administration console, perform the following:
1. Select the Advanced Tab.
2. Select the Security Tab.
3. Verify that “Security Mode” is configured to Hard. If it is not configured or set to soft, this is a finding.

Fixes: SUN0190 (Manual)

Configure Security Mode to Hard.

Vulnerability Key: V0016153

STIG ID: SUN0200
Release Number: 3
Status: Active
Short Name: No high availability for Sun Ray system configured
Long Name: The Sun Ray system is not configured for high availability.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0200
Severity: Category II
Long Name: The Sun Ray system is not configured for high availability.
Vulnerability Discussion: High availability is important when implementing the Sun Ray system since users authenticate and establish sessions with the Sun Ray servers. User data may also be stored on the Sun Ray server, and if this server should fail the entire user community will not be able to access the network. Providing a secondary server ensures the session and data availability for the user community.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

SUN0200 (Manual)

On the Sun Ray server perform the following:
/opt/SUNWut/sbin/utreplica -l

If no secondary failover servers are configured, this is a finding.

Fixes:

SUN0200 (Manual)

Configure the Sun Ray system with primary and secondary servers for failover.

Vulnerability Key: V0016155
STIG ID: SUN0210
Release Number: 3
Status: Active
Short Name: Failover group signature not configured
Long Name: A failover group signature is not configured on all Sun Ray servers in the failover group.

IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0210
Severity: Category II
Long Name: A failover group signature is not configured on all Sun Ray servers in the failover group.
Vulnerability Discussion: Without the use of a failover group signature, an unauthorized Sun Ray server may become a member of the group, thereby receiving replication traffic. Servers in a group authenticate one another using a common group signature. The group signature is a key used to sign messages sent between servers in a group, and it must be configured to be identical on each server.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0210 (Manual)

On the Sun Ray server, perform the following:
find /etc/opt/SUNWut/ -name gmSignature

If no results are returned, this is a finding.

Fixes: SUN0210 (Manual)

Configure a failover group signature to ensure only authorized servers are members of the group.

Vulnerability Key: V0016157
STIG ID: SUN0230
Release Number: 4
Status: Active
Short Name: Sun Ray Server does not record log files.
Long Name: The Sun Ray server does not record log files.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.4 Reporting
Effective Date: 15 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0230

Severity: Category II

Long Name: The Sun Ray server does not record log files.

Vulnerability Discussion: Logs form a recorded history or audit trail of the Sun Ray server system 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. Logging must be comprehensive to be useful for both intrusion monitoring and security investigations. Setting logging at the severity notice should capture most relevant events without requiring unacceptable levels of data storage. The severity levels notice and debug are also available to organizations that require additional logging for certain events or applications.

Responsibility: System Administrator
Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0230 (Manual)

1. Verify that syslogd is running on the system. Perform the following:
ps –ef | grep syslogd

If nothing is returned, this is a finding.

2. Verify /etc/syslog.conf is configured with the following entries:
cat /etc/syslog.conf
User.info /var/opt/SUNWut/log/messages
Local1.info /var/opt/SUNWut/log/admin_log

If these two entries are missing, this is a finding.

3. Critical Sun Ray log files are the administration, authentication, automatic mounting, mass storage devices, messages, and web administration. Significant activity is recorded in the following log files. Verify that these files are being written to by performing the following:

ls -Ll /var/opt/SUNWut/log | awk '{if ($5 ~ /^0$/ print}'

If any of the following log files are returned this is a finding.
admin_log
auth_log
utmountd.log
utstoraged.log
messages
utwebadmin.log

Example of log file with zero byte (0) size.
(i.e. –rw-r----- 1 root utadmin 0 Jun 29 utmountd.log)

If these logs are being written to an external syslog server, review that server to ensure the logs are being recorded.

Fixes: SUN0230 (Manual)
Record Sun Ray server activity to log files.

Vulnerability Key: V0016158
STIG ID: SUN0250
Release Number: 2
Status: Active
Short Name: Sun Ray server log permissions
Long Name: The Sun Ray server logs are more permissive than 640.
IA Controls: ECAN-1 Access for Need-to-Know
ECCD-1 Changes to Data
ECCD-2 Changes to Data
Categories: 2.1 Object Permissions
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0250
Severity: Category II
Long Name: The Sun Ray server logs are more permissive than 640.
Vulnerability Discussion: The Sun Ray server logs should be appropriately secured, having file permissions that restrict unauthorized changes or viewing. Unauthorized users accessing the audit logs may delete, modify, or change data within the logs for malicious purposes. Any alternation in the audit logs will not give the system administrator an accurate history of the events that occurred.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0250 (Manual)

On the Sun Ray server perform the following:

ls -al /var/opt/SUNWut/log | less

Log files that should be 640:
admin_log
auth_log
utmountd.log

utstoraged.log
messages
utwebadmin.log

If any of the audit log file permissions are greater than 640, this is a finding. If the audit logs are on an external syslog server, ensure permissions are 640. If they are not, this is a finding.

Fixes: SUN0250 (Manual)
Configure the Sun Ray server logs permissions to 640.

Vulnerability Key: V0016159
STIG ID: SUN0260
Release Number: 3
Status: Active
Short Name: Sun Ray audit logs are not retained
Long Name: The Sun Ray audit logs are not retained for a minimum of one year.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.5 Retention
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0260
Severity: Category II
Long Name: The Sun Ray audit logs are not retained for a minimum of one year.
Vulnerability Discussion: Storing log files for at least a year provides a way to recover these files in case an investigation is necessary. Typically these files are stored offline on tape media or external networks. 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 these 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. The Sun Ray audit logs should be appropriately backed-up and stored in order for them to be examined at a future time. If audit logs are unavailable to be viewed at a later time, system compromises and/or attacks will not be traceable. Therefore, Sun Ray audit logs will retained for a minimum of 1 year.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0260 (Manual)

Ask the IAO/SA where the Sun Ray system audit logs are stored. If they are offsite, review the process to move them to the alternative site. Verify that the audit data is retained for a minimum of one year by reviewing the dates of the oldest backup files or media. Audit data that should be retained include the following files on the Sun Ray server: (These files maybe at a different location for a remote syslog server.)

/var/opt/SUNWut/log/admin_log
/var/opt/SUNWut/log/auth_log
/var/opt/SUNWut/log/utmountd.log
/var/opt/SUNWut/log/utstoraged.log
/var/opt/SUNWut/log/messages
/var/opt/SUNWut/log/utwebadmin.log

Fixes: SUN0260 (Manual)
Retain all audit data for a minimum of one year.

Vulnerability Key: V0016349
STIG ID: SUN0270
Release Number: 2
Status: Active
Short Name: Sun Ray system backups are not performed
Long Name: The Sun Ray system backups are not performed in accordance with the assigned MAC level.
IA Controls: CODB-1 Data Back-up Procedures
CODB-2 Data Back-up Procedures
CODB-3 Data Back-up Procedures
Categories: 13.4 Backup & Recovery
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0270
Severity: Category II
Long Name: The Sun Ray system backups are not performed in accordance with the assigned MAC level.
Vulnerability Discussion: The three MAC level has different requirements for backing up data. For MAC III systems it is necessary to ensure that backups are performed weekly. For MAC II systems backups are performed daily and the recovery media is stored off-site in a protected facility in accordance with its mission assurance category and confidentiality level. In MAC I systems backups are maintained through a redundant secondary system, not colocated, and can be activated without loss of data or disruption to the operation. NOTE: The MAC level indicates the criticality of an asset to the DoD mission based on its purpose and user community. The Sensitivity level of an

asset must also be determined and is based on whether the data or resource is restricted or releasable to the public. There are three MAC and three Sensitivity levels. The MAC and Sensitivity level of the asset are an important factor in determining the security strength the access control solution must provide. MAC and Sensitivity Levels are further defined in Appendix C and DoDI 8500.2.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0270 (Manual)

1. Determine the MAC level of the Sun Ray system by asking the IAO/SA.
2. Once the MAC level is determined, locate the backup media or storage location.
For MAC I servers, a redundant secondary system is required that is not colocated.
For MAC II servers, daily backups are required with recovery media stored offline.
For MAC III servers, backups must be performed weekly.
3. Depending on the MAC level, verify the servers are backed up to media or storage within the guidelines of the MAC level. If they are not, this is a finding.

Fixes:

SUN0270 (Manual)

Backup the Sun Ray system in accordance to the MAC level.

Vulnerability Key: V0016351
STIG ID: SUN0310
Release Number: 3
Status: Active
Short Name: Admin password is not configured for Desktops
Long Name: Administrative password is not configured for Desktop Units.
IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication
Categories: 2.2 Least Privilege
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0310
Severity: Category II
Long Name: Administrative password is not configured for Desktop Units.
Vulnerability Discussion: From a physical security perspective, the DTU pop-menu is accessible, therefore a username/password or administrative only password is recommended to protect the device from unauthorized changes made locally.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0310 (Manual)

On the Sun Ray 2fs unit press the (Stop-M) on Sun Keyboard and on the PC keyboards press the (Ctrl-Pause-M or S).
If you are not prompted for a password to enter the firmware configuration, this is a finding. To configure the password, select Security, Password, and type in the password. Make sure it is compliant with DoD password policies.

Caveat: If the (Stop-M) on the Sun keyboard or the (Ctrl-Pause-M or S) on the PC keyboards does not bring up the pop-up firmware-gui, then the pop-up function is disabled for this firmware and this is not applicable.

Note: For other Sun Ray Desktop Units, consult the system administrator or documentation for the key mode combinations.

Fixes: SUN0310 (Manual)

Configure a username / password for the DTU pop-up menu.

Vulnerability Key: V0016354
STIG ID: SUN0320
Release Number: 3
Status: Active
Short Name: Sun Ray Desktop Units not assigned IP address
Long Name: Sun Ray Desktop Units are not assigned with DHCP reserved IP addresses.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 11 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0320

Severity: Category III

Long Name: Sun Ray Desktop Units are not assigned with DHCP reserved IP addresses.

Vulnerability Discussion: Sun Ray servers will not distribute DHCP addresses to non-Sun Ray Desktop Units. Configuring Sun Ray Desktop Units with reserved IP addresses will ensure no rogue desktop units are attached to the network and able to connect to the Sun Ray network. This will prevent unauthorized devices from receiving DHCP addresses from Sun Ray servers or external DHCP servers, and prevent access to the Sun Ray network.

Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks: SUN0320 (Manual)
Open the Solaris DHCP Manager or the DCHP server that is handing out IP addresses. The Solaris DHCP manager is located in /usr/sadm/admin/bin/dhcpmgr. Verify that the dynamic IP addresses are set to permanent or static based on the MAC.
Fixes: SUN0320 (Manual)
Configure Sun Ray session servers to reserve IP addresses for Desktop Units.

Vulnerability Key: V0016379
STIG ID: SUN0330
Release Number: 4
Status: Active
Short Name: There is no documented baseline of setuid/setgid
Long Name: There is no documented baseline of the default setuid and setgid files.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0330
Severity: Category II
Long Name: There is no documented baseline of the default setuid and setgid files.
Vulnerability Discussion: There are programs that have setuid and setgid flags set within the Sun Ray server. Setuid is a flag that allows an application to temporarily change the permissions of the user running the application by setting the effective user ID to the program owner's user ID. Setgid is a flag that allows an application to temporarily change the permissions of the group running the application by setting the effective group ID to the program owner's group ID. aseline of these applications will ensure that any unauthorized modifications to these files will detected. Several programs on the Sun Ray server have setuid and setgid flags installed by default. Disabling any of the setgid or setuid applications will result in problems with the Sun Ray system. Furthermore, having a documented baseline of these applications will ensure that any unauthorized modifications to these files will be detected.
Responsibility: System Administrator
Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

SUN0330 (Manual)

On the Sun Ray server perform the following:
find /opt –perm -4000

If the result does not return the following output only, this is a finding.

/opt/SUNWut/lib/utrcmd
/opt/SUNWut/lib/utguiauth
/opt/SUNWut/lib/utprefs-helper
/opt/SUNWut/lib/utdomount
/opt/SUNWut/bin/utaudio
/opt/SUNWut/bin/utxconfig

find /opt –perm -2000

If the result does not return the following output only, this is a finding.

/opt/SUNuttsc/lib/uttsc-bin

Ensure the documented setuid and setgid match the output above. If not, this is a finding.

Fixes: SUN0330 (Manual)

Document the setuid and setgid files on the Sun Ray system.

Vulnerability Key: V0016393
STIG ID: SUN0340
Release Number: 2
Status: Active
Short Name: Sun Ray server does not send logs to syslog server
Long Name: Sun Ray server does not send logs to syslog server.
IA Controls: ECAR-1 Audit Record Content
ECAR-2 Audit Record Content
ECAR-3 Audit Record Content
Categories: 10.4 Reporting
10.5 Retention
Effective Date: 11 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)
Policy: All Policies
MAC / Confidentiality Grid:

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

STIG ID: SUN0340

Severity: Category III

Long Name: Sun Ray server does not send logs to syslog server.

Vulnerability Discussion: Remote logging is essential in monitoring servers and detecting intrusion. If an intruder is able to obtain root on a host, they may be able to edit the system logs to remove all traces of the attack. If the logs are stored off the machine, they can be analyzed for suspicious activity and used for prosecuting the attacker. Centralized log monitoring and storage is a critical component of incident response and assuring the integrity of system logs.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0340 (Manual)

On the Sun Ray server, examine the /etc/syslog.conf file.
To send all syslog data from the Sun Ray server to a remote syslog host, search for the following line(s) in the /etc/syslog.conf file:
.<Tab><Tab> @loghost (name of remote host)

OR

*.debug, info, …@loghost

At a minimum, the following two log files must be configured to send their logs to a remote syslog server:

Log Name	Facility Level	Default Location
messages	user.info	/var/opt/SUNWut/log/messages
admin_log	local1.info	/var/opt/SUNWut/log/admin_log

Verify the loghost referred to in the syslog.conf file is not resolving to the localhost.
Check /etc/hosts file to review what the remote host is referring to. If it is not in this file, check the DNS server to determine what it is resolving to. If it is resolving to localhost, this is a finding.

Fixes:

SUN0340 (Manual)

Configure the Sun Ray server to send its logs to a remote syslog server.

Vulnerability Key: V0016394
STIG ID: SUN0370
Release Number: 3
Status: Active
Short Name: Sun Management Center does not monitor daemons
Long Name: The Sun Management Center does not monitor daemons, failover groups, and interconnects.
IA Controls: ECSC-1 Security Configuration Compliance
Categories: 12.4 CM Process
Effective Date: 11 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC /

	I - Mission Critical	II - Mission Support	III - Administrative

Confidentiality Grid:				
	Classified	☑	☑	☑
	Sensitive	☑	☑	☑
	Public	☑	☑	☑

STIG ID: SUN0370
Severity: Category II
Long Name: The Sun Management Center does not monitor daemons, failover groups, and interconnects.
Vulnerability Discussion: 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, starting, file changes, and so on. These changes may happen before the system administrator has time to review any logs.
Responsibility: Information Assurance Officer
References: Department of Defense Instruction 8500.2 (DODI 8500.2)
Checks:

SUN0370 (Manual)

Select the server that has the Sun Management Center software installed. Perform the following at the console:
/opt/SUNWsymon/sbin/es-start –c &
Enter the username/password and login
1. Select the Alarms tab.

2. Verify alarms are configured for the daemons, failover groups, and interconnects by performing the following:

a) Double-click on the Sun Ray Services icon on the left.
Daemons:
Dtlogin – Desktop login daemon
In.dhcpd – Dhcp daemon
Utauthd – Auth manager
Utdsd – Datastore daemon
Utsessiond – Session daemon
Utdevmgrd – Device manager

b) Double-click on the Sun Ray Failover Groups icon on the left.
failover Groups
primary and secondary servers

c) Double-click on the Sun Ray Interconnects icon on the left.
Interconnects (Network Interfaces Used by Sun Ray server):

If these are system objects are not configured with alarms, this is a finding.

Fixes:

SUN0370 (Manual)

Configure Sun Ray system in the Sun Management Center to monitor daemons, failover groups, and interconnects.

Vulnerability Key: V0016395
STIG ID: SUN0380
Release Number: 3
Status: Active
Short Name: Sun Ray server is not registered in VMS/database
Long Name: Sun Ray Server is not properly registered in VMS or database.
IA Controls: VIVM-1 Vulnerability Management
Categories: 12.5 IAVM Process
Effective Date: 12 Sep 2008

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

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0380

Severity: Category II

Long Name: Sun Ray Server is not properly registered in VMS or 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. As a result, 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 virtualization servers and resources, and supports a successful IAVM process. The ability to track assets improves the effective use of virtualization assets, information assurance auditing efforts, as well as optimizing incident response times.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0380 (Manual)

Access VMS or appropriate database and navigate to the site's assets. Ensure the Sun Ray Server(s) are registered within the database or VMS. If they are not registered, this is a finding.

Fixes: SUN0380 (Manual)

Register Sun Ray Servers in VMS or database.

Vulnerability Key: V0016396

STIG ID: SUN0390

Release Number: 4

Status: Active

Short Name: Sun Ray servers incorrectly configured in VMS

Long Name: Sun Ray servers are not configured with the correct posture in VMS.

IA Controls: VIVM-1 Vulnerability Management

Categories: 12.5 IAVM Process

Effective Date: 11 Sep 2008

☐ Open	Comments:

☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed	

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0390

Severity: Category II

Long Name: Sun Ray servers are not configured with the correct posture in VMS.

Vulnerability Discussion: Correctly configuring the Sun Ray asset 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: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks:

SUN0390 (Manual)

If VMS is used and check SUN0380 is a finding, this should be automatically marked as a finding.

If VMS is not being used, this is Not Applicable.

If the assets are registered in VMS, verify that the following postures are registered. If any of the postures are not registered this is a finding.

Solaris 10 or Red Hat Linux Advanced Server 4 or SuSE Linux Enterprise Server 9
Sun Ray 4
Tomcat 5.x

Fixes:

SUN0390 (Manual)

Register Sun Ray Servers in VMS with the correct posture.

Vulnerability Key: V0017455

STIG ID: SUN0400

Release Number: 2

Status: Active

Short Name: Sun Ray Server not in DMZ

Long Name: The Sun Ray Session Server (SRSS) is not located in a DMZ or screened subnet.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Effective Date: 09 Oct 2008

☐ Open ☐ Not a Finding ☐ Not Applicable	Comments:

Not Reviewed	

Condition: Sun Ray 4 (Target: Sun Ray 4)

Policy: All Policies

MAC / Confidentiality Grid:

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

STIG ID: SUN0400

Severity: Category II

Long Name: The Sun Ray Session Server (SRSS) is not located in a DMZ or screened subnet.

Vulnerability Discussion: If the SSRS is configured to service external clients from the internal enclave, there is a potential that an external adversary can obtain information about internal hosts that could assist the adversary in an attack. Firewalls, ACLs, and DMZs are used to enforce these types of restrictions and are components in the defense-in-depth architecture. The SRSS must be located in a protected DMZ if the server is servicing clients outside the local enclave. If the SrSS is only servicing clients inside the local enclave, then it must be behind the enclave and not part of the DMZ that houses public servers. Note: A DMZ is a physical or logical subnetwork that usually contains an organization's external services to a larger, untrusted network, typically the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). DoD Instruction 8500.2 requires a DMZ for confidentiality levels of High and Medium identified as classified and sensitive domains respectively. A DMZ provides boundary protection for architectures that interconnect enclaves.

Responsibility: Information Assurance Officer

References: Department of Defense Instruction 8500.2 (DODI 8500.2)

Checks: SUN0400 (Manual)

1. Validate the scope of clients that the Sun Ray Session Server (SRSS) is servicing. If the SRSS is servicing clients outside the local enclave, proceed to step 2. If the SRSS is servicing clients inside the local enclave, proceed to step 3.

2. The requirement is that the SRSS must be in a protected DMZ. Review the network topology diagram and obtain the SRSS IP address and subnet mask to validate that it is in the documented subnet for the DMZ. If no network topology diagram exists, work with the network reviewer/system administrator to determine if the SRSS is located in a DMZ. If it is not in a DMZ, this is a finding.

3. If the SRSS server is only serving clients inside the local enclave, the requirement is to be behind the enclave not part of the DMZ that houses the public servers. Review the network topology diagram and obtain the SRSS IP address and subnet mask to validate that it is in an enclave subnet for servers. If no network topology exists, work with the network reviewer/system administrator to determine where the SRSS server is located. If it is in the DMZ, this is a finding.

Fixes: SUN0400 (Manual)

Place the SRSS behind a screened subnet or DMZ.

Vulnerability Count - 29