Network Management
Internal Documentation

NA-CFG-30652 Iris Server Security Compliance and Validation Guide

Version 7.13.1

Tektronix®
communications

Internal Documentation—Confidential

Tektronix Communications
3033 W President George Bush Highway
Plano, Texas 75075
+1 469-330-4000 (voice)
www.tekcomms.com Web site

uadocfeedback@tek.com (Technical Publications email)

Plano, Texas USA - serves North America, South America, Latin America
+1 469-330-4581 (Customer Support voice)
uaservice@tek.com (Customer Support USA email)

London, England UK - serves Northern Europe, Middle East, and Africa
+44-1344-767-100 (Customer Support voice)
uaservice-uk@tek.com (Customer Support UK email)

Frankfurt, Germany DE - serves Central Europe and Middle East
+49-6196-9519-250 (Customer Support voice)
uaservice-de@tek.com (Customer Support DE email)

Padova, Italy IT - serves Southern Europe and Middle East
+39-049-762-3832 (Customer Support voice)
uaservice-it@tek.com (Customer Support IT email)

Melbourne, Australia - serves Australia
+61 396 330 400 (Customer Support voice)
uaservice-ap@tek.com (Customer Support Australia and APAC email)

Singapore - serves Asia and the Pacific Rim
+65 6356 3900 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Tektronix Communications, Inc. Proprietary Information
001-130628 **NA-CFG-30652 Iris Server Security Compliance and Validation Guide**

The products and specifications, configurations, and other technical information regarding the services described or referenced in this document are subject to change without notice. All statements, technical information, and recommendations contained in this document are believed to be accurate and reliable but are presented “as is” without warranty of any kind, express or implied. Users must take full responsibility for their application of any products specified in this document. Tektronix Communications, Inc. makes no implied warranties of merchantability or fitness for a purpose as a result of this document or the information described or referenced within, and all other warranties, express or implied, are excluded.

Except where otherwise indicated, the information contained in this document represents the planned capabilities and intended functionality offered by the product and version number identified on the front of this document. Screen images depicted in this document are representative and intended to serve as example images only. Wherever possible, actual screen images are included.

Table of Contents

Revision History

Table 1 - Current Release

Version	Date	Reason and Sections Updated
1.0	2013-05-31	Split the SNMP default configuration vulnerability into two items, one for Iris Alarms and the other for the Solaris SNMP service.
1.0	2013-05-30	**Single source two security documents from this set of FrameMaker files:** • NA-CFG-30649 SpIserver Security Compliance and Validation Guide • NA-CFG-30652 Iris Server Security Compliance and Validation Guide Iris server and SpIserver unique elements are conditional text with color backgrounds. Import settings for each document from a file containing the correct FrameMaker variables and Conditional Text Hide/Show settings.
1.0	2013-05-23	Change compliance from **full** to **partial** for security vulnerabilities related to account umask permissions.
1.0	2013-05-21	Initial Draft of Security Hardening Document based on the F-01628 Technology Refresh Feature

1.0 Introduction

1.1 Overview

As part of the Technology Refresh initiative, developers analyzed security issues related to the Iris Server and produced recommendations that describes security hardening necessary for the server.

1.2 Scope

The security violations fixed in code or by upgrading web containers are covered under the Technology Refresh requirements (F-01628) for Apache HTTP Server, Apache Tomcat, and JBoss and are *not* part of this document.

Security hardening procedures, for example, disabling Telnet, FTP, TFTP daemon reflect the core content of this document. The PRD also lists reference documents that have been produced for internal consumption in the past for legacy UA and UACN/RIA (in the references section of the PRD).

In some cases, this document may required services to be disabled that our software needs to function correctly, for example, SNMP mail daemon. This security compliance and validation document will explain that the service is required for the correct operation of the product.

1.3 How to Use This Document

Use **Table 1.1, Iris Server Security Vulnerabilities** to look up a specific security vulnerability. Click a hyperlink in the table to go to the document section for instructions on how to:

- Check vulnerability for current status with Tektronix security standards.
- Perform procedures necessary steps to secure the SpIserver.
- Run commands that validate full or partial compliance with these security standards.

1.4 Assumptions

When a service is necessary for the correct operation of the server and the Tektronix applications, that service will remain active.

1.5 The Meaning of Compliance in this Document

The server will be in **Full, Partial**, or **No Compliance** with each security issue.

- **Full compliance**—Product does not make use of the concerned item, such as `rsh`.
- **Partial compliance**—Product has a feature that needs the item, but can be disabled along with feature loss. Alternatively, could require manual configuration to bring the product or feature into compliance.
- **No compliance**—Product relies on the particular item and cannot be disabled without impacting the system.

If a security issue is categorized as **Partial Compliance** or **No Compliance**, potential impacts to the server should be provided here for actions taken by the customer IT department that could potentially affect the Tektronix software solution, for example, implementing access white lists at a firewall.

1.6 Iris Server Security Vulnerabilities Identified

Security vulnerabilities are organized into groups in the next section of the document. In **Table 1.1, Iris Server Security Vulnerabilities**, they are listed by title in alphabetical order. Use the **Table 1.1, Iris Server Security Vulnerabilities** or the document **Index** to quickly locate answers to questions about these server security issues.

Table 1.1 - Iris Server Security Vulnerabilities

Security Issue Short Title	[Compliance Level] Security Vulnerability
Application and services start/stop limited to system administrators	**[Full]** Access permission over start/stop application/service shall be limited to system administration function only.
Buffer overflow prevented in dstpcd service	**[Full]** Disable `dstpcd` service running on the server.
Cross Site Request Forgeries (CSRF) prevented	**[No]** Cross Site Request Forgeries (CSRF) are an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. If the targeted end user is the administrator account, this can compromise the entire web application.
Cross Site Scripting Attacks (CSSA) prevented	**[Full]** Cross-site scripting (XSS) exploits where input passed using an HTML request that is not properly sanitized before being displayed to the user, whereby an attacker could potentially insert arbitrary HTML and script code that runs in a user's browser session.
Default OS built-in accounts disabled (exclude super user account)	**[Full]** All commands must be run under the super user account.
Default umask permission secure	**[Partial]** Default `umask` permission shall be set to **027** or more secure setting.
Disable accounts used for application connectivity or OS from user access	**[Full]** User accounts used for application or system connecting or system operating shall be prohibited for carbon-based life form login.
Home directories’ permission secured	**[Full]** Home directories’ permission shall be set to **750** or more secure setting.

Table 1.1 - Iris Server Security Vulnerabilities (Continued)

Security Issue Short Title	[Compliance Level] Security Vulnerability
Prohibit IP packet forwarding	**[Full]** Disable all IP packet forwarding
Logs do not receive transactions from remote servers	**[Full]** Log receiving transaction from other servers shall be prohibited (except the server used for centralized log keeping).
Login attempts (failures) limited	**[Full]** Number of failed logins shall be limited to five (5) attempts.
Login inactive session feature enabled	**[Full]** Enable the inactive login session feature. This includes a password required for a resumed session with a secure shell or screen saver.
Login (remote) using powerful system accounts disabled	**[Full]** Highest powerful system account e.g. root and local administrator shall be prohibited for remote login.
Login warning messages enabled	**[Full]** The warning messages during the login process shall be enabled.
Network packet capture limited to administrators only	**[Full]** Authority over captured network package at local network interface shall be limited to administration function only.
New password does not match previously used five passwords	**[Full]** User cannot reuse any of the previous five (5) passwords for setting a new password.
Oracle access through tnslsnr service eliminated	**[Full]** A sever with the Oracle `tnslsnr` service running can allow an attacker to see the exact Oracle version in use. An attacker can also use SQL SQL injection. It is recommended to filter incoming traffic for just the authorized machines.
Oracle database auditing disabled	**[Full]** Refer to `http://www.oracle.com/technetwork/database/security/index.html` for more Oracle administration details.
Oracle password policy settings strong	**[Partial]** The Oracle users of `geo` default must not be edited, such as `geo`, `uacommon`, `OPS$BIA`, and so forth.
Oracle remote login settings strong	**[Full]** Do not permit remote Oracle account logins.
Oracle resource settings adequate	**[Partial]** Inadequate resource utilization settings. Reassign Oracle users from the default profile to a new Oracle user profile.
Oracle role (SYSDBA and SYSOPER) auditing disabled	**[Full]** Auditing of SYSDBA and SYSOPER roles disabled
Oracle users with Connect and Resource Privileges revoked	**[Full]** Users with Connect and Resource Privileges Refer to `http://www.oracle.com/technetwork/database/security/index.html` for more Oracle administration details.
Oracle users with unlimited Tablespace privilege changed	**[Full]** Revoke `UNLIMITED TABLESPACE` privilege from a new user. It is dangerous because this privilege gives rights to write in any Tablespace the user chooses to, including the `SYSTEM` Tablespace.
Enforce strong password creation	**[Full]** Password complexity enforcement shall be implemented and include: • character • numeric • special character
Password expiration interval	**[Full]** Password expiration interval shall be set less than or equal to 30 days for all enabled carbon-based life login accounts.

Table 1.1 - Iris Server Security Vulnerabilities (Continued)

Security Issue Short Title	[Compliance Level] Security Vulnerability
Password length enforced	**[Full]** Minimum password length shall be eight (8) characters.
Password cannot be null or blank	**[Full]** Null or blank password shall be prohibited.
Password mandatory for user account switching	**[No]** Password shall be required as a mandatory for switching to other user accounts.
Remote access authority limited	**[Full]** Remote access authority shall be granted to user accounts based upon need-to-do basis. The list of granted authority user account shall be documented.
Remote access for root login disabled	**[Full]** `ssh` to your regular user account, then use `su` or `sudo` to become **`root`** for specific tasks. Remote access for `root` user is disabled by default on Solaris. Do not enable it. For check and fix, see [Login (remote) using powerful system accounts disabled]
Remote login rlogin service disabled, encrypted services used	**[Full]** `rlogin` running on the system, `.rhost` file present on the system. `rlogin` does not use encryption and all the traffic is sent in plain text. Recommend disable the `rlogin` service and use encrypted services `slogin` or `ssh` instead.
Remote mountable NFS shares secured	**[Full]** It is possible to access NFS without credentials and mount it on an attacking machine. An attacker can use it for reading and possibly writing stored files on this machine.
Restart and shut down authority limited	**[Full]** Restart and shut down system authority shall be limited to administration function only.
Root account has strong default umask value set	**[Partial]** Change the account `umask` may affect the installation) It is recommended to configuring the `umask` for the root account to 077 (only accessible for `root`), for the other accounts to at least 027.
RPC Service disabled to secure passwords	**[Full]** The `RPC BOOTPARAMD` service has a vulnerability in providing information. When an attacker uses `BOOTPARAMPROC_WHOAMI` and provides the exact client address, it can obtain the NIS domain and easily obtain the NIS password file.
Sensitive files and high-privilege commands limited	**[Full]** Permission over sensitive files and usage of high privilege commands shall be limited to system administration only. • UNIX based OS, that is, stored password file, network configuration file, and user profile file. • Windows files, that is, stored password file; and high-privilege commands for all platforms: start/stop service, generate log, change system policy, user account management, and network configuration.
Security ticket (Kerberos) lifetime less than 600 minutes	**[Full]** The maximum Kerberos ticket lifetime shall be set to 600 minutes.
Security log access limited to administrative security	**[Full]** Access permission over security log files limited to security administration function only.
Services/protocols, disable insecure and unnecessary ones	**[Full]** Unnecessary and insecure services/protocols, for example, WWW, FTP, Finger, and Telnet shall be disabled.

Table 1.1 - Iris Server Security Vulnerabilities (Continued)

Security Issue Short Title	[Compliance Level] Security Vulnerability
SNMP configuration secure	**[Full]** It is recommended that default community strings should not be used for SNMP. See [SNMP service `write` permission is disabled] to check and fix.
SNMP Alarms service not disabled	**[Partial]** The Tektronix customized SNMP *must not* be disabled. Tektronix SNMP service for Alarms *cannot* be disabled.
SNMP Solaris default service disabled	**[Full]** Tektronix Simple Network Management Protocol (SNMP) service for Alarms cannot be disabled. Disable Solaris default SNMP service on the remote host or at least change the default community string. (See **SNMP service write permission is disabled** to secure necessary data.)
SNMP service write permission is disabled	**[Full]** Write community string should be restricted as it allows changing SNMP MIB data on the remote server.
SSH set higher than version Two	**[Full]** Secure shell protocol shall be set to version 2 or higher.
Strong password encryption used	**[Full]** Password stored in the system shall be encrypted with strong algorithm, that is, SHA-512, MD5, or NT hash at a minimum.
System access .rhosts, .shosts, and .netrc files restricted to administration staff	**[Full]** The trusted host and user shall be limited properly based upon need-to-do basis`.rhosts` or `/etc/hosts.equiv` files.
System logs enabled to audit key events	**[Full]** These system logs shall be enabled: • Login and logout both successful and fail events • User account maintenance, that is, add, delete, and modify account authority; • System event, for example, service start/stop, hard disk full, service error, system error, and so forth • System and security policy change (for Windows).
Tomcat administration restricted to localhost	**[Full]** It is recommended to restrict access of Tomcat manager application to localhost only
Tomcat - Inadequate Shutdown attribute set	**[Full]** Default WebCT Tomcat opens the remote shut down in 8005.
Unique account names, UIDs, and GIDs	**[Full]** Unique identification, user identifiers (UIDs), group identifiers (GIDs), and account names shall be implemented.
JBoss website uses non-default user name and password	**[Full]** Administration interface for JBOSS (`http://<address>/web-console/`) has the default credentials: user: admin and password: admin.
Weak passwords for users identified and changed	**[Full]** Users with weak password are always a top IT security risk. Use safe passwords according to the company's policy and change the default password encryption algorithm.
XDMCP service disabled	**[Full]** XDMCP service is inherently insecure and should be used in trusted networks (corporate network within a firewall). Never use it in the open network (or Internet) environment without a firewall protection! Consider using alternatives feature such as Nomachine NX, which is a secure version of X. Disable XDMCP service running on the server.

2.0 Security Vulnerabilities

2.1 Overview

Each security vulnerability section:

- Describes the security issue
- How to check for it’s existence
- Steps to remedy the situation
- Provides notes and advice
- Lists tests that validate compliance with the Tektronix standard

Each security issue has a compliance classification:

- (**Full**)—Full Compliance
- (**Partial**)—Partial Compliance
- (**No**)—No Compliance

This section divides the server security issues into these groups

- **Oracle Database Security Issues**
- **Password Security Issues**
- **Remote Access to Server Security Issues**
- **User Login and Account Security Issues**
- **SNMP Security Issues**
- **Website Security Issues**
- **Audit and Transaction Log Security Issues**
- **Miscellaneous Security Issues**

2.2 Oracle Database Security Issues

Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities. Iris server Oracle security issues include:

- **Oracle access through tnslsnr service eliminated**
- **Oracle password policy settings strong**
- **Oracle resource settings adequate**
- **Oracle role (SYSDBA and SYSOPER) auditing disabled**
- **Oracle users with Connect and Resource Privileges revoked**
- **Oracle users with unlimited Tablespace privilege changed**

2.2.1 Oracle access through tnslsnr service eliminated

Description **[Full]** Detected that the machine has a Oracle `tnslsnr` service running. This product allows an attacker to see the exact version being used. Also an attacker can use SQL sql injection. It is recommended to filter incoming traffic for just the authorized machines.

Assess Security Issue

All commands must be run under the `oracle` account. (This account is created during `INETstuls` package installation.)
Connect to Oracle DB from a host which is not supposed to have access to the DB.

```
sqlplus /nolog (run from shell on intruder host)
CONNECT irisowner/iris@//<Oracle DB hostname>:1521/IRIS Connected
Connected
```

Fix Security Vulnerability

1. Go to `$ORACLE_HOME/network/admin` and add the following lines to the `sqlnet.ora` file.

   ```
   tcp.validnode_checking = yes
   tcp.invited_nodes = (localhost,hostname,example1,example2,example3,…)
   ```

   Note: Blank spaces before and after the = sign are mandatory.

   ```
   where:
   localhost  Always mandatory,
   hostname   DNS localhost name with the Oracle DB installed
   ```

   `example1/2/3/…` All hosts with Iris applications which require access to the Oracle DB.
   Pure IPv4 address can be specified if necessary (example 134.64.206.168)

2. Stop and start the `lsnrctl` listener service:

   ```
   LSNRCTL> stop
   LSNRCTL> start
   ```

3. Check connection to the Oracle DB from the authorized hosts (tcp.invited_nodes).
   For example:

   ```
   sqlplus /nolog (run from shell on sh-uacn1 host = localhost)
   CONNECT irisowner/iris@//localhost:1521/UA
   Connected
   ```

Compliance Test

4. Check there is no connection from non-authorized host. For example:

   ```
   sqlplus /nolog (run from shell on sh-spi05 host)
   CONNECT irisowner/iris@//berna-vm2:1521/IRIS
   ERROR:
   ```

5. `ORA-12537: TNS:connection closed`Check all Iris web applications (OAM, UUMS, and so forth) work as expected.

2.2.2 Oracle password policy settings strong

Description **[Partial]** Tektronix does not recommend external changes in the Iris Oracle database. Refer to http://www.oracle.com/technetwork/database/security/index.html for additional details about addressing Oracle security vulnerabilities. Iris applications use Oracle accounts such as `ISAOWNER`, `ITAOWNER`, and `IRISUSER` to connect to the Oracle database. These Iris users belong to the default profile and the profile should never be changed with the password security setting. For example, setting the `PASSWORD_LIFE_TIME: 60` parameter, causes the account to lock and Iris application stops working after 60 days.

Caution

All commands must be run under the `oracle` account. This account is created after the Iris server installation.

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check the compliance run:

```
SYS@iris> SELECT USERNAME, PROFILE FROM DBA_USERS;
```

These Oracle users are **`iris` default accounts** and *must not be changed*:

```
USERNAME           PROFILE
--------------------------
APPQOSSYS          DEFAULT
ANONYMOUS          DEFAULT
BO_REPORTS         DEFAULT
BO_DASH            DEFAULT
BO_AUDITO          DEFAULT
COGNOSOWNER        DEFAULT
CTXSYS             DEFAULT


DIP                DEFAULT
DBSNMP             DEFAULT
HEALTHOWNER        DEFAULT
IRISGUEST          DEFAULT
IRISOWNER          DEFAULT
IRISUSER           DEFAULT
ISAOWNER           DEFAULT


ITAOWNER           DEFAULT
MDSYS              DEFAULT
ORACLE_OCM         DEFAULT
ORDDATA            DEFAULT
ORDPLUGINS         DEFAULT
ORDSYS             DEFAULT
OUTLN              DEFAULT


PORTOWN1           DEFAULT
SI_INFORMTN_SCHEMA DEFAULT
SYS                DEFAULT
SYSTEM             DEFAULT
TPADMIN1           DEFAULT


TPAPP1             DEFAULT
TPKEYHOLE1         DEFAULT
TPOWNER1           DEFAULT
XDB                DEFAULT
```

According to Iris version and components installed (GEO, RIA, Touchpoint, and so forth) there may be more Iris users in the list for your server or in the future. Tektronix highly recommends you do not use the Oracle Iris DB for anything else. You need to check what are the default `iris` users after each Iris installation or upgrade. Isolate these accounts from any possible modifications.

Compliance Test

To check for compliance run this SQL command:

```
SQL> SELECT USERNAME, PROFILE FROM DBA_USERS;
```

Fix Security Vulnerability

Refer to Oracle Database Security Guide for information how to design your own verification function. Then reassign the user to the profile:

```
ALTER USR testusr PROFILE tek_profile;
```

If you find other users they should be reassigned from `DEFAULT` profile to the new one.
Create (or alter) the profile and set password policy using these commands:

```
SQL> CREATE PROFILE tek_profile LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_REUSE_MAX 12
PASSWORD_LOCK_TIME 60
PASSWORD_VERIFY_FUNCTION <your verify function>
FAILED_LOGIN_ATTEMPTS 3;
```

Then reassign the user to the profile.

2.2.3 Oracle resource settings adequate

Description **[Partial]** Tektronix does not recommend external changes in the Iris Oracle database. Tektronix recommends limiting the database resources that can be used by regular end users, also set the following parameters within the profile of regular users to an adequate level. Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities. Iris applications use Oracle accounts such as `ISAOWNER`, `ITAOWNER`, and `IRISUSER` to connect to the Oracle database. These Iris users belong to the default profile and the profile should never be changed. Profile changes can cause applications to stop working.

Caution

All commands must be run under the `oracle` account. This account is created after the Iris server installation.

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check the compliance run:

```
SYS@iris> SELECT USERNAME, PROFILE FROM DBA_USERS;
```

These Oracle users are **`iris` default accounts** and *must not be changed*:

```
USERNAME            PROFILE
--------------------------
APPQOSSYS           DEFAULT
ANONYMOUS           DEFAULT
COGNOSOWNER         DEFAULT
CTXSYS              DEFAULT
DIP                 DEFAULT
DBSNMP              DEFAULT
HEALTHOWNER         DEFAULT


IRISGUEST           DEFAULT
IRISOWNER           DEFAULT
IRISUSER            DEFAULT
ISAOWNER            DEFAULT
ITAOWNER            DEFAULT
MDSYS               DEFAULT
ORACLE_OCM          DEFAULT
```

```
ORDDATA            DEFAULT
ORDPLUGINS         DEFAULT
ORDSYS             DEFAULT
OUTLN              DEFAULT
SI_INFORMTN_SCHEMA DEFAULT
SYS                DEFAULT
SYSTEM             DEFAULT


XS$NULL            DEFAULT
XDB                DEFAULT
```

According to Iris version and components installed (GEO, RIA, Touchpoint, and so forth) there may be more Iris users in the list for your server or in the future. Tektronix highly recommends you do not use the Oracle Iris DB for anything else. You need to check what are the default `iris` users after each Iris installation or upgrade. Isolate these accounts from any possible modifications.

Fix Security Vulnerability

Refer to Oracle Database Security Guide for information how design the verification function. Then reassign the user to the profile:

```
ALTER USR testusr PROFILE tek_profile;
```

If you find other users they should be reassigned from `DEFAULT` profile to the new one.
Create (or alter) the profile and set password policy using these commands:

```
SQL@iris> CREATE PROFILE tek_profile LIMIT
CPU_PER_SESSION <value>
CPU_PER_CALL <value>
PRIVATE_SGA <value>
SESSIONS_PER_USER <value>
LOGICAL_READS_PER_CALL <value>
LOGICAL_READS_PER_SESSION <value>
CONNECT_TIME <value>
IDLE_TIME <value>;
```

The value to set depends on your needs. Then reassign the user to the profile.

2.2.4 Oracle role (SYSDBA and SYSOPER) auditing disabled

Description **[Full]** Disable auditing of the SYSDBA and SYSOPER Oracle roles. Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities.

Compliance Test

All commands must be run under the `oracle` account. (This account is created after Iris server installation)

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check for compliance:

```
SQL@iris> show parameter AUDIT_SYS_OPERATIONS;
NAME                 TYPE    VALUE
-------------------- -------------
audit_sys_operations boolean FALSE
```

Fix Security Vulnerability

1. 1. Set TRUE for the parameter
   ```
   SQL@iris> ALTER SYSTEM SET audit_sys_operations=TRUE COMMENT='Begin auditing
   SYS' SCOPE=SPFILE;
   System altered
   ```
2. Stop the Oracle DB
   ```
   SQL@iris> shutdown immediate
   Database closed.
   Database dismounted.
   ORACLE instance shut down
   ```
3. Start the Oracle DB
   ```
   SQL@iris> quit;
   Disconnected
   oracle@sh-uacn3:~$ sqlplus / as sysdba (example)
   ```
4. Connected to an idle instance.
   ```
   SQL@iris> startup
   ORACLE instance started
   ```

2.2.5 Oracle users with Connect and Resource Privileges revoked

Description **[Full]** Tektronix recommends to review connect and resource privilege granted to various database users and if not required, revoke these privileges from the users profile.

Compliance Test

All commands must be run under the oracle account. (This account is created after Iris server installation.)

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
SQL@iris> select * from dba_role_privs where GRANTED_ROLE = 'RESOURCE';
GRANTEE                GRANTED_ROLE ADM DEF
---------------------- ------------ --- ---
CTXSYS                 RESOURCE     NO
LOGSTDBY_ADMINISTRATOR RESOURCE     NO  YES
MDSYS                  RESOURCE     NO
OUTLN                  RESOURCE     NO
SYS                    RESOURCE     YES
XDB                    RESOURCE     NO

SQL@iris> select * from dba_role_privs where GRANTED_ROLE = 'CONNECT';
GRANTEE           GRANTED_ROLE ADM DEF
------------      ------------ --- ---
COGNOS_OWNER_ROLE CONNECT      NO  YES
COGNOS_USER_ROLE  CONNECT      NO  YES
HEALTH_USER_ROLE  CONNECT      NO  YES
HEALTH_OWNER_ROLE CONNECT      NO  YES
IRIS_GUEST_ROLE   CONNECT      NO  YES
IRIS_OWNER_ROLE   CONNECT      NO  YES
IRIS_USER_ROLE    CONNECT      NO  YES


ISA_OWNER_ROLE    CONNECT      NO  YES
ISA_USER_ROLE     CONNECT      NO  YES
ITA_OWNER_ROLE    CONNECT      NO  YES
ITA_USER_ROLE     CONNECT      NO  YES
MDSYS             CONNECT      NO  YES
SYS               CONNECT      YES YES
TPADMIN1          CONNECT      YES YES
```

Fix Security Vulnerability

If the privileges are not required then run these commands

```
SQL@iris> revoke RESOURCE from testusr;
Revoke succeeded
SQL@iris> revoke CONNECT from testusr;
Revoke succeeded
```

and grant privileges that for the oracle account needed.

2.2.6 Oracle users with unlimited Tablespace privilege changed

Description **[Full]** This privilege gives rights to write in any Oracle Tablespace the user chooses—even in the SYSTEM Tablespace. Administrators should revoke the `UNLIMITED TABLESPACE` privilege from any new user. Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities.

Compliance Test

All commands must be run under the oracle account. (This account is created after Iris server installation.)

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check the compliance and ensure that there are no unwanted users assigned to the privilege.
By default there is an *exception to this security rule for these users:*

```
SQL@iris> select * from dba_sys_privs where PRIVILEGE = 'UNLIMITED
TABLESPACE';
GRANTEE                PRIVILEGE            ADM
---------------------- ------------------------
CTXSYS                 UNLIMITED TABLESPACE NO
DBA                    UNLIMITED TABLESPACE YES
DBSNMP                 UNLIMITED TABLESPACE NO
LOGSTDBY_ADMINISTRATOR UNLIMITED TABLESPACE NO
MDSYS                  UNLIMITED TABLESPACE NO
OPS$BIA                UNLIMITED TABLESPACE NO
OPS$ORACLE             UNLIMITED TABLESPACE NO


ORDSYS                 UNLIMITED TABLESPACE NO
OUTLN                  UNLIMITED TABLESPACE NO
SI_INFORMTN_SCHEMA     UNLIMITED TABLESPACE NO
SYS                    UNLIMITED TABLESPACE NO
SYS                    UNLIMITED TABLESPACE NO
SYSTEM                 UNLIMITED TABLESPACE YES
TPADMIN1               UNLIMITED TABLESPACE NO
XDB                    UNLIMITED TABLESPACE NO
```

Fix Security Vulnerability

After granting `RESOURCE` role to any new user (for example, `testusr`) you should run this command:

```
SQL@iris> revoke unlimited tablespace from testusr;
Revoke succeeded.
```

Now grant quotas on tablespaces that you want for this user.

2.3 Password Security Issues

Iris server password security issues include:

- **Enforce strong password creation**
- **Password expiration interval**
- **Strong password encryption used**
- **Password length enforced**
- **Password cannot be null or blank**
- **Password mandatory for user account switching**
- **New password does not match previously used five passwords**
- **Weak passwords for users identified and changed**

2.3.1 Enforce strong password creation

Description **[Full]** Enforce strong password creation by including a combination of the these elements in the required user passwords:

- alphanumeric characters
- numeric numbers
- a least one special character

Assess Security Issue

To check run this command:

```
> cat /etc/default/passwd
```

and check parameters listed in the fixing security vulnerability section.

Fix Security Vulnerability

Set the `MINALPHA`, `MINDIGIT`, and `MINSPECIAL` parameter values in the `/etc/default/passwd` file to:

```
MINALPHA=1
MINDIGIT=1
MINSPECIAL=1
```

2.3.2 Password expiration interval

Description **[Full]** The password expiration interval shall be set less than or equal to 30 days for all enabled carbon-based life form login accounts.

Assess Security Issue

To check run this command:

```
> cat /etc/default/passwd
```

and check parameter in the fix security vulnerability section.

Fix Security Vulnerability

Set the `MAXWEEKS` parameter value in the `/etc/default/passwd` file to:

```
MAXWEEKS=4
```

2.3.3 Strong password encryption used

Description **[Full]** Passwords stored in the system shall be encrypted with a strong algorithm, that is, SHA-512, MD5, and NT hash at a minimum.

Assess Security Issue

Run this command:

```
> cat /etc/security/policy.conf
```

Fix Security Vulnerability

Set the cryptography parameter in the `/etc/security/policy.conf` file to:

```
CRYPT_DEFAULT=6
CRYPT_ALGORITHMS_DEPRECATE=_unix_
```

2.3.4 Password length enforced

Description **[Full]** The password length shall be set to at least eight (8) characters.

Assess Security Issue

Run this command:

```
> cat /etc/default/passwd
```

and check parameter in the Fix Security Vulnerability area that follows.

Fix Security Vulnerability

Set the value of the `PASSLENGHT` parameter in the `/etc/default/passwd` file to:

```
PASSLENGHT=8
```

2.3.5 Password cannot be null or blank

Description **[Full]** A null or blank password must be prohibited.

Assess Security Issue

1. To ensure the installed system has no user account with a null password in the `/etc/shadow` file, use this command:

   ```
   > cut -f 1 -d : /etc/passwd | xargs -i passwd -s {} | grep -in NP
   ```

   If the user account has null password, output `NP` is shown.

   Note: For Solaris 11 there could be warning messages displayed to the console: `"WARNING: changing account in reserved uid range: daemon"`. You can ignore these messages.

2. To check that all accounts require passwords:

   ```
   > grep PASSREQ /etc/default/login
   ```

   The output for compliance should be:

   ```
   PASSREQ=YES
   ```

3. To check for null password compliance in SSH server logins:

   ```
   > grep PermitEmptyPasswords /etc/ssh/sshd_config
   Output should be:
   PermitEmptyPasswords no
   ```

Fix Security Vulnerability

1. To remove the null password user account, the required password value in the `/etc/default/login` file shall be set to:
   ```
   > passwd <user_name>
   ```
2. If a null password is found for an account, just set `PASSREQ=YES` in the `/etc/default/login` file
3. To prevent any server login through SSH with a user account containing null password, set the value of the `PermitEmptyPasswords` parameter in the`/etc/ssh/sshd_config` file to:
   ```
   setting:PermitEmptyPasswords no
   ```

2.3.6 Password mandatory for user account switching

Description **[No]** A password shall be mandatory for switching between user accounts. Most of `iris` aliases (for example, `irStopAc`) use `sudo`. Currently only `oracle` and `iris` users are allowed to `sudo` without a password.

Assess Security Issue

Check if some users can run `sudo` without the changing passwords with this command:

```
> grep NOPASSWD /opt/sfw/etc/sudoers
```

Fix Security Vulnerability

If the issue exists, comment out all violations in the `/opt/sfw/etc/sudoers` file with these commands:

```
# iris    ALL=(ALL)        NOPASSWD:ALL
# oracle    ALL=(ALL)        NOPASSWD:ALL
```

2.3.7 New password does not match previously used five passwords

Description **[Full]** Reusing the last five previous passwords shall be prohibited when a user creates a new password.

Assess Security Issue

Run these commands:

```
> cat /etc/default/passwd
> ls -la /etc/security/passhistory
```

and check parameter in the fix security vulnerability section.

Fix Security Vulnerability

The value of `HISTORY` parameter in the `/etc/default/passwd` file shall be set to:

```
HISTORY=5
```

Notes

If the `/etc/security/passhistory` file does not exist, the file shall be created with proper detail of account and authority. The 500 mode shall be assigned to the system file. The owner and the owner's group shall be assigned to `'root'` and `root`, respectively as shown in these commands:

```
> cd /etc/security
> touch passhistory
> chmod 500 passhistory
> chown root:root passhistory
```

2.3.8 Weak passwords for users identified and changed

Description **[Full]** Users with weak password are always one of the top IT security risks. Use safe passwords according to company policy and change the default password encryption algorithm. The default UNIX encryption algorithm can handle only the first 8 password symbols and thus has a potential vulnerability. For example, user `iris` with a set password `123456789abcd` can successfully login using `12345678` or `123456789a` as a password.

Fix Security Vulnerability

See **Enforce strong password creation**
See **Password expiration interval**
See **Password length enforced**
See **Login attempts (failures) limited**
See **New password does not match previously used five passwords**
See **Strong password encryption used**

Notes

Remember the `root` password does not follow this policy. The restrictions mentioned in the previous links work only if a non-`root` user changes its own password.

2.4 Remote Access to Server Security Issues

Iris server remote access security issues include:

- **Login (remote) using powerful system accounts disabled**
- **Remote access authority limited**
- **Remote access for root login disabled**
- **Remote login rlogin service disabled, encrypted services used**
- **Remote mountable NFS shares secured**

2.4.1 Login (remote) using powerful system accounts disabled

Description **[Full]** The most powerful system accounts, for example, `root` and local administrator shall be prohibited from logging in remotely.

Assess Security Issue

Run these commands:

```
> cat /etc/default/login
> cat /etc/ssh/sshd_config
```

and check the parameters in the next fix security vulnerability section.

Fix Security Vulnerability

1. The `root` account shall be prohibited from direct remote logging by using the `/etc/default/login` file by commenting out the "#" character in the file line:
   `CONSOLE=/dev/console`
2. For the SSH service, set the `PermitRootLogin` parameter value in the `/etc/ssh/sshd_config` file to:
   `PermitRootLogin no`

2.4.2 Remote access authority limited

Description **[Full]** Remote access authority shall be granted to user accounts based on a “need-to-do-work” basis. The list of granted authority user accounts shall be documented.

Fix Security Vulnerability

1. All unauthorized user for FTP service shall be prohibited by adding prohibited user accounts to the `/etc/ftpd/ftpusers` file (one user account per line):

Example:

```
# ident "@(#)ftpusers   1.5     04/02/20 SMI"
#
# List of users denied access to the FTP server.
#
root
iris
oracle
geo
testuser
```

2. All unauthorized user for SSH service shall be prohibited by adding prohibited users to the `DenyUsers` parameter in the `/etc/ssh/sshd_config` file, similar to this setting:
`DenyUsers` *`<user_name1> <user_name2> <user_name3>`*

Example:

```
...
DenyUsers oracle geo iris testuser
...
```

2.4.3 Remote access for root login disabled

Description **[Full]** compliant Use `ssh` to access your regular user account, then use `su` or `sudo` to become the `root` user for specific administration tasks. Remote access for `root` user is disabled by default on Solaris and should be never enabled.

Assess Security Issue

See **Login (remote) using powerful system accounts disabled**.

Fix Security Vulnerability

See **Login (remote) using powerful system accounts disabled**.

2.4.4 Remote login rlogin service disabled, encrypted services used

Description **[Full]** Rlogin does not use encryption and all the traffic is sent in plain text. Disable the `rlogin` service and use `slogin` or `ssh` encrypted services instead.

Assess Security Issue

All commands must be run under the super user account. To check rlogin service status, run this command:

```
> svcs  -a | grep -i rlogin
```

Fix Security Vulnerability

Disable and stop the service, use this command:

```
> svcadm disable rlogin
```

2.4.5 Remote mountable NFS shares secured

Description **[Full]** It is possible to access NFS without credentials, and it's possible to mount it on an attacking machine. An attacker can use it for reading (and possibly writing) files stored on this machine. Because the port is greater than 1024, a user does not need `root` privileges to mount the shared directory. It is recommended to configure NFS on the remote host so that only authorized hosts can mount the remote shares. The remote NFS server should prevent mount requests originating from a non-privileged port.

Assess Security Issue

1. Check if the NFS service is running:
```
> svcs -a | grep -i /network/nfs/server
```
2. Check if there are any permanent shares configured:
```
> cat /etc/dfs/dfstab
```

Fix Security Vulnerability

Configure NFS for authorized hosts only. There are two ways to share folders on the server:

- Run shell command `share [-F fstype] [-o options] [-d "<text>"] <pathname> [resource]` . This command does not persist over reboots.
- Set that share command entry in the `/etc/dfs/dfstab` system file.

In both cases the `share` command must be specified with the following options:

1. `rw=client[:client]...`

   Pathname is shared read/write only to the listed clients. No other systems can access pathname. Do not use `rw` without the list of clients. Try to avoid granting write permissions.

2. `ro=client[:client]...`

   Pathname is shared read only to the listed clients. No other systems can access pathname. Do not use `ro` option without the list of clients.

3. Never use `root=... option` . It defines which host has `root` access to this specific NFS share.

4. Use `nosub` option if applicable.

   Means that only the exported directory can be mounted by a client host, disables direct mounting of subdirectories.

5. Use `root_squash` option if applicable.This prevents `root` users connected remotely from having root privileges. Instead, the NFS server assigns them the user ID `nfsnobody`. This effectively eliminates the power of the remote `root` user to the lowest local user, preventing possible unauthorized writes on the remote server.

Notes

1. `rw` option has higher priority then `ro` option.

   Thus `-o rw=hostA`, `ro=hostA` gives read/write permissions to `hostA`.

2. Be careful with host names, sometimes it is needed to set host name FQDN.
   For example:

```
> share -F nfs -o ro=devosa-vm2 /export0/home/testuser/tshare
```
   Result: permission from `devosa-vm2` denied.

```
> share -F nfs -o ro=devosa-vm2.rich.tek.com /export0/home/testuser/tshare
```
   Result: Only connection from `devosa-vm2` is allowed.

Compliance Test

After NFS configuration using `/etc/dfs/dfstab`, restart the service and check that only authorized hosts can mount remote shares.

2.4.6 Oracle remote login settings strong

Description **[Full]** Remove weak remote login settings. Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities.

Compliance Test

All commands must be run under the `oracle` account. (This account is created after Iris server installation.)

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check for strong remote access compliance:

```
SQL> show parameter REMOTE_LOGIN_PASSWORDFILE;
NAME                         TYPE    VALUE
------------------------- ------ -----
remote_login_passwordfile string NONE
```

Fix Security Vulnerability

1. 1. Set NONE for the parameter.

```
SYS@iris>   ALTER SYSTEM SET remote_login_passwordfile= NONE COMMENT='Secure
DB' SCOPE=SPFILE;
System altered.
```

2. Stop the Oracle database.

```
SYS@iris> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
```

3. Start the Oracle database.

```
SYS@iris> quit; Disconnected
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> conn /as sysdba
Connected to an idle instance
```

4. Start the Oracle database.

```
SYS@iris> startup
ORACLE instance started
```

2.5 User Login and Account Security Issues

Iris server user login and account security issues include:

- **Default OS built-in accounts disabled (exclude super user account)**
- **Default umask permission secure**
- **Disable accounts used for application connectivity or OS from user access**
- **Home directories' permission secured**
- **Login attempts (failures) limited**
- **Login inactive session feature enabled**
- **Login warning messages enabled**
- **Unique account names, UIDs, and GIDs**

2.5.1 Default OS built-in accounts disabled (exclude super user account)

Description **[Full]** All default operating system built-in accounts shall be disabled, excluding the super user account.

Assess Security Issue

All commands must be run under the super user account.
To check run this command:

```
> grep /bin/false /etc/passwd
```

If there is an output for a user, the user account is disabled.

If not, you must repair the security vulnerability for these default operating system built-in accounts: **daemon**, **bin**, **sys**, **adm**, **lp**, **uucp**, **nuucp**, **smmsp**, **listen**, **nobody**, **nobody4**, and **noaccess**.

Fix Security Vulnerability

Solaris 10

To fix the default operating system built-in accounts, disable them with these commands:

```
> passwd -l  <user_name>
> usermod -s /bin/false <user_name>
```

A script to disable the default operating system build-in accounts would look like:

```
# LIST="daemon bin sys adm lp uucp nuucp smmsp listen nobody nobody4 noaccess”
for USERS in $LIST; do
  passwd -l $USERS
  usermod -s /bin/false $USERS
done
```

Solaris 11

All build-in accounts are read-only (by default) and you do not need to disable them with the script.

Notes

Output password information unchanged is not a problem.

2.5.2 Default umask permission secure

Description **[Partial]** Set the default `umask` permission to `027` or a more secure setting.

Compliance Test

Fix Security Vulnerability

1. Set the default permission value of the `umask` parameter in these files to `027`:
   ```
   /etc/profile
   ~root /.profile
   $HOME/.profile
   ```
2. Set the default permission value of the `umask` parameter in the `/etc/default/login` file to:
   ```
   UMASK 027
   ```

2.5.3 Disable accounts used for application connectivity or OS from user access

Description **[Full]** User accounts for the application/system connecting or system operating shall be prohibited for carbon-based life form logins.

Assess Security Issue

All commands must be run under the super user account.

```
> grep /bin/false /etc/passwd
```

Find user account used for application or system functions only in the output.

Fix Security Vulnerability

To restrict login for user account used for application/system functions, type this command:

```
> usermod -s /bin/false <user_name>
```

Notes

Users `iris` and `oracle` should not be altered:

- `iris` can be used by `runIrisCli` and used for Iris server management.
- `oracle` can be used for Oracle DB management.

2.5.4 Home directories’ permission secured

Description **[Full]** Set home directories' permission to 750 or a more secure setting.

Compliance Test

Use these commands to find all regular users and their home directories:

```
> cat /etc/passwd
# ls -la <user home directory>
```

Check that the home directory permission is set to `drwxr-x---`

Fix Security Vulnerability

Set the home directory to `750` mode using this command:

```
> chmod 750 <user home directory>
```

Notes

These commands are applicable only for regular accounts, not system default accounts.
That is, a `root` user with an `/` home directory exists; but it is an error to set `750` permissions to the `/` directory.

2.5.5 Login attempts (failures) limited

Description **[Full]** Limit the maximum number of failed login attempts to five attempts.

Assess Security Issue

Run this command to check security:

```
> cat /etc/default/login
> cat /etc/security/policy.conf
> cat /etc/ssh/sshd_config
> cat /etc/user_attr
```

and check the parameters in the Fix Security Vulnerability area that follows.

Fix Security Vulnerability

1. Set the `RETRIES` parameter value to five (5) in `/etc/default/login` file:
   ```
   RETRIES=5
   ```
2. Set the `LOCK_AFTER_RETRIES` parameter value in `/etc/security/policy.conf` file to:
   ```
   LOCK_AFTER_RETRIES=YES
   ```
3. Set the `MaxAuthTries` parameter value in the `/etc/ssh/sshd_confi` file to:
   ```
   MaxAuthTries 5
   ```

Notes

To disable lock after retries for user `root`, set the `lock_after_retries` parameter value in the `/etc/user_attr` file to **no**, if it exists:

```
root:::type=role;auths=solaris.*,solaris.grant;lock_after_retries=no;
```

2.5.6 Login inactive session feature enabled

Description **[Full]** The inactive login session feature shall be enabled including password required on the resumed session for secure shell and screen saver.

Compliance Test

All commands must be run under the super user account. If the timeout is set to less than 900, it is also applicable. Nine hundred is a recommended value; you can set any value according to your administrative and security guidelines.

To check for inactive session compliance:

```
# grep TIMEOUT /etc/default/login
```

check value of 900

```
# grep TMOUT /etc/profile
```

check value of 900

```
# grep LoginGraceTime /etc/ssh/sshd_config
```

check value of 900

```
# find /usr/dt/config -name sys.resources
```

Check the value of the `dtsession*saverTimeout` and `dtsession*lockTimeout` parameters in the `/usr/dt/config/*/sys.resources` file have the values:

```
dtsession*saverTimeout: 15
dtsession*lockTimeout: 15
```

If you do not find a file, you do not need no vulnerability fix

Fix Security Vulnerability

Solaris 11

Find all `.xscreensaver` files to set default locking screen saver with this command:

```
<hostname>#find / -name .xscreesaver:
timeout:         0:10:00
cycle:           0:10:00
lock:            True
lockTimeout:     0:00:00
passwdTimeout:   0:02:00
passwdTimeoutEnabled:True
```

Solaris10

1. Find all sys.resources files to set default locking screen saver with this command:

   ```
   <hostname># find /usr/dt/config -name sys.resources
   ```

2. The value of `dtsession*saverTimeout` and `dtsession*lockTimeout` parameter shall be set in `/usr/dt/config/*/sys.resources` file as shown in this setting:

   ```
   dtsession*saverTimeout: 15
   dtsession*lockTimeout: 15
   ```

3. Set the time out parameter values in these files using these parameter-value pairs:

   ```
   /etc/default/login file as: TIMEOUT=900
   /etc/profile' file as: TMOUT=900
   ```

4. When the user account requires an Inactive session, set the `TMOUT` parameter to `TMOUT=900` in the /`USER HOME>/profile` file. You should document each exception with the appropriate reason and detail the exception in the remark section of an implementation sheet.
5. Set the unsuccessful login grace period for a user account in the `/etc/ssh/sshd_config` file to a 15 minute maximum:

   ```
   LoginGraceTime 900
   ```

6. Restart the Service Secure Shell using this command:

   ```
   > svcadm restart svc:/network/ssh:default
   ```

2.5.7 Login warning messages enabled

Description **[Full]** The server shall enable he warning messages during the login process. An example warning banner displays:

Notes

All the configuration files listed in this security issue must be updated using the standard vi editor provided by Solaris command line utility. **Warning**: after you copy-and-paste the text in the insert mode you must delete symbols ' and type the same symbol from the keyboard. Otherwise the text will be displayed incorrectly. After the changes are made, all involved services must be restarted or reboot the server.

Also edit the `/etc/ssh/sshd_config` file to display the warning message and make this setting:

```
# Banner to be printed before authentication starts.
Banner /etc/issue
```

Assess Security Issue

The warning banner shall be set for SSH using the `/etc/issue` file with the following statement:

```
All materials in the Company’s Information System including all relevant, documents are taken
as assets belonging to Total Access Communication Public, Company Limited. Such Company’s and
customers’ materials are considered confidential. All rights are reserved. No person may use
these materials for other purposes except for the use of the Company’s business. The
reproduction, modification, access and dissemination of all materials by any means without
permission or authorization from the Company are prohibited. Any violations will result in
reserves the right to prosecute to the maximum extent possible.
```

Fix Security Vulnerability

Solaris 10:

1. For the warning banner for **FTP** to edit `/etc/ftpd/banner.msg` file or banner parameter in the `/etc/ftpd/ftpaccess` file with statement as **'Authorized person access only'** to display the warning message to the remote user before authentication shall be set. Also banner option can be set like:

```
banner /etc/ftpd/banner.msg
```

2. To fix the issue the warnings banner for **Telnet** `/etc/default/telnetd` file to display the warning message to the remote user before authentication shall be set the `BANNER` parameter with statement to **'Authorized person access only'**. Furthermore, the authority of the file shall not be granted to higher mode than `444`. The owner and the owner group of the file shall be set to `root` and `sys`, respectively.

```
# ls -la /etc/default/telnetd
-r-- r-- r-- 1 root   sys      542 Jan 15 04:34 /etc/default/telnetd
```

Solaris 11:

3. Add warning banner message to /etc/issue file and run this command:

```
# echo "DisplayConnect /etc/issue" >> /etc/proftpd.conf
```

4. For the warning banner for **mail service** in `/etc/mail/sendmail.cf` file to display the warning message to the remote user using the **'O SmtpGreetingMessage'** parameter shall be set the statement to **'Authorized person access only'**.

   To check mail service banner:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 Authorized ESMTP person access only
```

(Word ESMTP set automatically)

5. After the change to the `sendmail.cf` file, restart the SMTP service using the command:

```
> svcadm restart svc:/network/smtp:sendmail
```

Notes

For Solaris 11, the server takes the warning banner from the `/etc/issue` file and so the steps for the FTP and Telnet services are not required.

2.5.8 Unique account names, UIDs, and GIDs

Description **[Full]** The server shall implement unique identification in the form of User IDs (UID), group IDs (GID), and account names.

Assess Security Issue

Verify unique GIDs and UIDs exist in the `/etc/passwd` and `/etc/group` files using these commands:

1. Verify duplicate UIDs.

```
> cut -f 3 -d : /etc/passwd | uniq -d
```

   If row returns more than 0 items, duplicate UIDs were found.

2. Verify duplicate GIDs.

```
> cut -f 3 -d : /etc/group | uniq -d
```

   If row returns more than 0 items, duplicate GIDs were found.

3. Verify duplicate account names.

```
> cut -f 1 -d : /etc/passwd | uniq -d
```

   If row returns more than 0 items, duplicate account names were found.

Fix Security Vulnerability

Remove duplicate UID and GIDs using these commands:

```
> userdel <user_name>
> grouprdel <group_name>
```

2.6 SNMP Security Issues

Iris server SNMP security issues include:

- **SNMP configuration secure**
- **SNMP Solaris default service disabled**
- **SNMP Alarms service not disabled**
- **SNMP service write permission is disabled**

2.6.1 SNMP configuration secure

Description **[Full]** It is recommended that default community strings should not be used for SNMP.

Assess Security Issue

See **SNMP service write permission is disabled**.

Fix Security Vulnerability

See **SNMP service write permission is disabled**.

2.6.2 SNMP Solaris default service disabled

Description **[Full]** Recommend you disable Solaris default SNMP service on the remote host or at least change the default community string (see **SNMP service write permission is disabled**) to secure necessary data.

Assess Security Issue

All commands must be run under the super user account
To check the SNMP service status, run this SMF command

```
> svcs  -a | grep -i snmp
```

Fix Security Vulnerability

For Solaris 10

Stop the service using these commands:

```
> cd /etc/init.d
> ./init.dmi stop
> ./init.snmpdx stop
> ./init.sma stop
```

And disable the services, use these commands:

```
> svcadm disable dmi
> svcadm disable snmpdx
> svcadm disable sma
```

For Solaris 11

Stop the service using this command:

```
> /etc/rc3.d/S82net-snmp stop
```

And disable the service using this command:

```
> svcadm disable svc:/application/management/net-snmp:default
```

Notes

To restart the Tektronix SNMP service after stopping it:

```
> /etc/rc3.d/S82net-snmp start
```

2.6.3 SNMP Alarms service not disabled

Description **[Partial]** The Tektronix customized SNMP *must not* be disabled. Tektronix SNMP service for Alarms *cannot* be disabled.

Compliance Test

1. To check the status of the Iris SNMP *receiver,* get the value of the following server plist:
   `plists.com.tektronix.iris.server.alarms.alarmcollector\collectors\<collectorId>\snmpReceiverEnabled`

Set the value=`true,` otherwise the Iris server cannot *receive* alarms from TD140 probes.

2. To check the status of Iris SNMP *sender,* get the value of the following server plist:
   `plists.com.tektronix.iris.server.alarms.alarmcollector\snmpProcessor\snmpProcessingEnable`

Set the value=`true,` otherwise the server cannot *forward* alarms to an external NMS (such as NetCool).

2.6.4 SNMP service write permission is disabled

Description **[Full]** The Write permission for the SNMP remote access service shall be prohibited. The Write community string must be restricted to prevent changing SNMP MIB data on the remote server.

Assess Security Issue

All commands must be run under the super user account.

Solaris 10:

Search for the write entry in the `/etc/snmp/conf/snmpd.conf` file.

```
> grep write /etc/snmp/conf/snmpd.conf
```

Solaris 11:

Search for the write entry in the `/etc/net-snmp/snmp/snmpd.conf` file.

```
> grep write /etc/net-snmp/snmp/snmpd.conf
```

Fix Security Vulnerability

Solaris 10:

Comment out all write permission of SNMP service in the `/etc/snmp/conf/snmpd.conf` file.
The `catd@dm1n` is example community string.

```
#tem-group-write-community catd@dm1n
#write-community catd@dm1n
```

Solaris 11:

Comment out all write permission of SNMP service in the `/etc/net-snmp/snmp/snmpd.conf` file.
The `catd@dm1n` is example community string.

```
#tem-group-write-community catd@dm1n
#write-community catd@dm1n
```

2.7 Website Security Issues

Iris server Tomcat and JBoss web server security include:

- **Tomcat administration restricted to localhost**
- **Tomcat - Inadequate Shutdown attribute set**
- **JBoss website uses non-default user name and password**
- **Cross Site Request Forgeries (CSRF) prevented**
- **Cross Site Scripting Attacks (CSSA) prevented**

2.7.1 Tomcat administration restricted to localhost

Description **[Full]** Restrict access to the Tomcat manager application only to the localhost. In the default IRIS server installation, the Tomcat manager application is not deployed.

Assess Security Issue

In a browser navigate to the URL `<hostname>:8080/manager/text/list`. Ensure that a 404 response is received. Do not access the login form, as it would be in fresh Tomcat installation.

Fix Security Vulnerability

The best solution is to remove the Tomcat manager deployment, since it is not needed for Iris Server.

1. Stop the corresponding Tomcat service.
2. Remove the `/home/iris/tomcat/webapps/manager` directory.

2.7.2 Tomcat - Inadequate Shutdown attribute set

Description **[Full]** Default Tomcat settings allow remote shutdown by sending `SHUTDOWN` to 8005 port (`<Server port="8005" shutdown="SHUTDOWN">`). No actions required for security hardening in a default iris server installation. All Tomcat configurations files (`tcInstances/IRIS_MAIN/conf/server.xml`, `IRIS/conf/server.xml`, `IPI/conf/server.xml`) have `<Server port="-1">`. (See Fix Security Vulnerability.)

Compliance Test

To check compliance that the port is disabled:

```
> netstat -an | grep 8005
```

Fix Security Vulnerability

Change the `$HOME/tomcat/site/server.xml` configuration files and set `port` attribute of <Server> element to -1 (`<Server port="-1">`).

2.7.3 JBoss website uses non-default user name and password

Description **[Full]** Administration interface for JBoss in this URL:(`http://<address>/web-console/`) has the default credentials of `user: admin`, `password: admin`. Change the default password.

Compliance Test

Browse these Internet links and attempt to login as `user: admin` and with the `password: admin`.

```
http://<Iris Server hostname>:8080/web-console
http://<Iris Server hostname>:8080/jmx-console
```

Notes For the Iris JBoss web and JMX console, `admin/admin` are not the default credentials. These credentials are set in the Derby DB and stored as encrypted strings. After an Iris JBoss installation, the default credentials are `admin/TEKENC(3425de6bdd83598898a0298969ad809e)`.

2.7.4 Cross Site Request Forgeries (CSRF) prevented

Description **[No]** The Iris Server is vulnerable, no way to protect existing installation without upgrading and to fix the issue. CSRF means crafting and transmitting malicious links from attacker to authorized user, and tricking an authorized user to click them. For example, malicious links can be hidden within a picture in e-mail or on a web page.

Assess Security Issue

Deleting a G10 Probe as an example of unauthorized action. The corresponding request URL is `http://<hostname>:8080/irisOAMWeb/probe/deleteProbe/?id=<id> http://localhost:8080/irisOAMWeb/probe/deleteProbe/?id=4105`
(Ensure, that server `<hostname>` is up and running, and that probe `<id>` exists and is offline).

1. Login to Iris Server.
2. Put the above URL into an e-mail.
3. Click the URL from the e-mail.
4. Make sure that the probe is deleted.

Fix Security Vulnerability

Tektronix will need to upgrade Iris and introduce a session management token for all HTTP requests.

2.7.5 Cross Site Scripting Attacks (CSSA) prevented

Description **[Full]** Cross Site Scripting (XSS) means injecting malicious scripts into an Internet page, that will later are displayed by victimized site. (**1**) Non-persistent XSS attacks can be executed, if some HTTP request renders a page. When the HTTP request renders one of request parameters as text (for example, a search form) without escaping special characters. In that case, an XSS vector (such as `<script>[malicious code here]</script>` or `<p onmouseover=[malicious code here]>[some text here]</p>`) can be passed as a parameter to the HTTP request. In IRIS server web interface, no such forms exist - all HTTP requests, that render a page, don't have any parameters. (2) A persistent XSS can be executed when some input form does not properly validate the input, and input results are displayed as plain text on some page. In this case, a malicious user can inject XSS vector into input. Later, another user displays the page, and the script executes in the browser.

Notes

Most of ExtJS widgets have an internal XSS prevention mechanism (escaping special characters when they are displayed), except for grids, which are said to be vulnerable. Also, self-made widgets could be vulnerable. However, excessive testing did not find any vulnerable components.

Assess Security Issue

1. Find an HTTP request with parameters, that renders a page (such as `http://[hostname]:8080/irisOAMWeb/oamDash/main`), and renders one of its parameters as text. If such request exists (most likely, it does not exist), try to use a test XSS vector in one of parameters (such as `<script>alert('XSS')</script>` or `<p onmouseover=alert('XSS')>[some text here]</p>`). Make sure, that script is not executed, that is, the alert window does not display.
2. Try injecting some test XSS vector (see above for example) into an input field. Make sure, that in resulting page the script is not executed. Also, check other pages, where your input field is also displayed. on all of that pages script should not be executed.

Fix Security Vulnerability

When the issue is discovered, it will require a software enhancement to implement parameter validation and proper text escaping.

2.8 Audit and Transaction Log Security Issues

Iris server audit security log issues include:

- **Oracle database auditing disabled**
- **Logs do not receive transactions from remote servers**x
- **Security log access limited to administrative security**
- **Application and services start/stop limited to system administrators**

2.8.1 Oracle database auditing disabled

Description **[Full]** Disable auditing of the Oracle database. Refer to **http://www.oracle.com/technetwork/database/security/index.html** for additional details about addressing Oracle security vulnerabilities.

Compliance Test

All commands must be run under the `oracle` account.

```
oracle@berna-vm2:/export/oracle > sqlplus /nolog
@> connect /as sysdba
```

To check compliance, use this command:

```
SQL@iris> show parameter AUDIT_TRAIL;
NAME          TYPE   VALUE
--------------------------
audit_trail   string NONE
```

Fix Security Vulnerability

1. Set `DB` or `DB,EXTENDED` for the parameter
   ```
   SQL@iris> ALTER SYSTEM SET audit_trail=DB COMMENT='Begin auditing SYS'
   SCOPE=SPFILE;
   System altered
   ```
2. Stop the Oracle DB
   ```
   SQL@iris> shutdown immediate
   Database closed
   Database dismounted
   ORACLE instance shut down
   ```
3. Start the Oracle DB
   ```
   SQL@iris> quit;
   Disconnected
   oracle@berna-vm2:/export/oracle > sqlplus /nolog
   @> connect /as sysdba
   ```
4. Connected to an idle instance.
   ```
   SQL@iris> startup
   ORACLE instance started
   ```

2.8.2 Logs do not receive transactions from remote servers

Description **[Full]** Logs receiving transaction from other servers shall be prohibited, except for the server used for centralized log keeping.

Compliance Test

```
> grep LOG_FROM_REMOTE /etc/default/syslogd
```

Check `NO` is set.

```
> cat /etc/default/sendmail
```

Check `MODE=Ac` and `QUEUEINTERVAL=15m` are set.

Fix Security Vulnerability

1. Set the value of `LOG_FROM_REMOTE` parameter in the `/etc/default/syslogd` file to:
   ```
   LOG_FROM_REMOTE=NO
   ```
2. Restart the service
   ```
   > svcadm restart svc:/system/system-log:default
   ```
3. Set the values to disable received mail for another host in the `/etc/default/sendmail` file to:
   ```
   MODE=Ac
   QUEUEINTERVAL=15m
   ```
4. If there is no `/etc/default/sendmail` file, then create the file.
5. Stop and restart the `sendmail` service
   ```
   > /etc/init.d/sendmail stop
   > /etc/init.d/sendmail start
   ```

2.8.3 Security log access limited to administrative security

Description **[Full]** Access permission over security log files shall be limited to security administrators. May require manual configuration.

Compliance Test

1. Check access to the superuser actions monitoring log:
   ```
   > ls -la /var/adm/sulog
   The output in case of compliance should be something like:
   -rw-------  root     root       39526 Jan 16 04:06 /var/adm/sulog
   ```

2. Check access to the login actions monitoring log:
   ```
   > ls -la /var/adm/loginlog
   The output in case of compliance should be something like or no file exists:
   -rw-------  1 root   sys        0 Jan 15 05:24 /var/adm/login
   ```

3. Check access to daily report files:
   ```
   > ls -la /var/adm | grep -w acct
   The output in case of compliance should be something like:
   drwxrwx---  5 adma   dm         512 May 162011 acct
   ```

Fix Security Vulnerability

1. Set the permission, owner, and group owner of the `/var/adm/sulog` file to `600` mode, `root`, and `root`, respectively with these commands:
   ```
   <hostname>#chown root:sys /var/adm/sulog
   <hostname>#chmod 600 /var/adm/sulog
   ```

2. Set the permission, owner, and group owner of the `/var/adm/loginlog` file to `600` mode, `root`, and `sys`, respectively with these commands:
   ```
   <hostname>#chown root:sys /var/adm/loginlog
   <hostname>#chmod 600 /var/adm/loginlog
   ```

3. Set the permission, owner, and group owner of the `/var/adm/acct` file to `600` mode, `adm`, and `adm`, respectively with these commands:
   ```
   <hostname>#chown adm:adm /var/adm/acct
   <hostname>#chmod 770 /var/adm/acct
   ```

2.8.4 System logs enabled to audit key events

Description **[Full]** Enable these system logs to audit critical server events:

- Login and logout, successful and failed attempts
- User account maintenance, that is, add, delete, and change account authority
- System events, for example, service start/stop, hard disk full, service error, system error, and so forth
- System and security policy change (for Windows)

Fix Security Vulnerability

1. Set the `SYSLOG` parameter value in the `/etc/default/login` file to:
   ```
   SYSLOG=YES
   ```

2. Set the value of access control logging in the `/etc/syslog.conf` file with these setting: (add `cron` and `auth` entry to the existing one):
   ```
   *.err;kern.notice;auth.n /dev/sysmsg
   *.err;kern.debug;daemon.notice;mail.crit;cron.info;auth.info /var/adm/messages
   ```

3. Check that system log service is online:

```
> svcs  -a | grep -i system-log
```

4. Set the value of `MaxAuthTriesLog`, `LogLevel`, and `SyslogFacility` parameters in the `/etc/ssh/sshd_config` file using these settings:

```
MaxAuthTriesLog 5
LogLevel INFO
SyslogFacility AUTH
```

5. Set the value of the `CRONLOG` parameter in the `/etc/default/cron` file to this setting:

```
CRONLOG=yes
```

Notes

Log example from `/var/adm/messages`:

```
...
Jan 15 06:15:20 berna-vm2 sshd[26456]: [ID 800047 auth.info] Accepted
keyboard-interactive for iris from 10.250.158.32 port 63820 ssh2
Jan 15 06:24:16 berna-vm2 ftpd[28077]: [ID 532633 daemon.notice] FTP LOGIN
REFUSED (username in /etc/ftpd/ftpusers)
FROM berna-vm2 [10.250.155.146], iris
```

2.9 Miscellaneous Security Issues

Iris server security issues that remain unclassified include:

- **Application and services start/stop limited to system administrators**
- **Buffer overflow prevented in dstpcd service**
- **Network packet capture limited to administrators only**
- **Prohibit IP packet forwarding**
- **Restart and shut down authority limited**
- **Root account has strong default umask value set**
- **RPC Service disabled to secure passwords**

- **Sensitive files and high-privilege commands limited**
- **Security ticket (Kerberos) lifetime less than 600 minutes**
- **SSH set higher than version Two**
- **Services/protocols, disable insecure and unnecessary ones**
- **System access .rhosts, .shosts, and .netrc files restricted to administration staff**

- **XDMCP service disabled**

2.9.1 Application and services start/stop limited to system administrators

Description **[Full]** Limit access permission over starting and stopping applications (and services) to system administrators.

Notes All commands must be run under the super user account. Round brackets must be specified with leading \ symbol.

Compliance Test

```
> find /etc/rc* /etc/init.d -type f -a ( ! -user root -o ! -group sys )
> find /etc/rc* /etc/init.d -type f -a ( -perm -002 -o -perm -022 -o -perm -020
-o -perm -001 )
```

Fix Security Vulnerability

Use these commands:

```
> find /etc/rc* /etc/init.d -type f -a ( ! -user root -o ! -group sys ) -exec
chown root:sys {} \;
> find /etc/rc* /etc/init.d -type f -a   ( -perm -002 -o -perm -022 -o -perm -
020 -o -perm -001 ) -exec chmod 754 {}\;
```

2.9.2 Buffer overflow prevented in dstpcd service

Description **[Full]** The `dtspcd` service has a buffer overflow vulnerability. This service is used along with CDE interface for the X11 system. Disable the `dstpcd` service running on the server.

Assess Security Issue

All commands must be run under the super user account.
To check the status of the `dtspcd` service:

```
> ps -ef | grep dtspcd
```

Fix Security Vulnerability

1. Comment out the `dtspcd` entry in the `/etc/inetd.conf` file.
2. Kill and restart the `inetd` daemon:
   ```
   > ps -ef | grep inetd
   > kill -HUP <inetd PID>
   ```
3. Run this command:
   ```
   > inetadm | grep dtspcd
   ```
4. If the service is "enabled", then disable it:
   ```
   > inetadm -d dtspcd
   ```
5. Ensure `dtspcd` entry is commented out in `/etc/services` file.

2.9.3 Network packet capture limited to administrators only

Description **[Full]** Authority over network packet capture at local network interface shall be limited only to administrators.

Assess Security Issue

The permission, owner, and group owner of the `/usr/sbin/snoop/` file shall be set to `550` mode, `root` and `bin` respectfully.
To check compliance, check the files permissions are `r-xr-x---`

```
> ls -la /usr/sbin/snoop
```

Fix Security Vulnerability

To remove the vulnerability, use these commands:

```
> chmod 550 /usr/sbin/snoop
> chown root:bin /usr/sbin/snoop
```

2.9.4 Prohibit IP packet forwarding

Description **[Full]** IP packet forwarding shall be prohibited.

Compliance Test

To check the compliance, run the script

```
> ls -la /etc/rc3.d/S99netconfig
```

Fix Security Vulnerability

Solaris 10

Create the file `/etc/rc3.d/S99netconfig` using this script:

```
#!/bin/bash
# IP packet forwarding shall be prohibited.
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip6_forward_src_routed 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip6_ignore_redirect 1
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip ip6_strict_dst_multihoming 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip6_send_redirects 0
```

Solaris 11, add these additional commands to the script:

```
routeadm -d ipv4-forwarding -d ipv6-forwarding
routeadm -d ipv4-routing -d ipv6-routing
```

Run these commands to set ownership and permissions for the script:

```
> chmod 740 /etc/rc3.d/S99netconfig
> chown root:root /etc/rc3.d/S99netconfig
```

This script runs every time the server reboots, making IP restrictions permanent.

2.9.5 Restart and shut down authority limited

Description **[Full]** Restart and shut down system authority shall be limited to administrators. Only root account should stop, start and reboot the server.

Assess Security Issue

The permission, owner, and group owner of these files shall be set to `550` mode, `root` and `root`, respectively. Check files permissions are `r-xr-x---` with this command:

```
> ls -la /usr/sbin/shutdown /usr/sbin/init /usr/sbin/halt /usr/sbin/reboot
/usr/sbin/poweroff
```

Fix Security Vulnerability

Fix the security vulnerability with these commands:

```
> chmod 550 /usr/sbin/shutdown /usr/sbin/init /usr/sbin/halt /usr/sbin/reboot
/usr/sbin/poweroff
> chown root:root /usr/sbin/shutdown /usr/sbin/init /usr/sbin/halt
/usr/sbin/reboot  /usr/sbin/poweroff
```

2.9.6 Root account has strong default umask value set

Description **[Partial]** Changing the account `umask` may affect the installation. It is recommended to configuring the `umask` for the `root` account to 077 (only accessible for `root`), for the other accounts to at least **`027`**. If you apply the umask value before Iris installation, QA should test this procedure.

Notes

Bash shell users can work with this example. (The same approach can be applied for csh users using the `/etc/.login` configuration file)
First find out the full path to the `whoami` shell command. Edit the `/etc/profile` file and

Solaris 10 default path: `` ACCOUNT=`/usr/ucb/whoami` ``

Solaris 11 default path: `'/usr/bin/whoami'`

Assess Security Issue

Login as `root` and other active user accounts and run

```
> umask
022
```

Fix Security Vulnerability

1. Add the following script to the `/etc/.login` file:

```
set ACCOUNT = `/usr/ucb/whoami`
if ($ACCOUNT == "root") then
   umask 077
else
   umask 027
endif
```

2. Save the file, re-login, and run once again:

```
# su -
# umask
077
```

or

```
# su - iris
# umask
027
```

Notes

As a user can overwrite the `umask` setting, editing of user shell configuration scripts (such as, `.profile`, `.kshrc`, `.login`, `.bash_profile`, `.bashrc`, `.cshrc`, and so forth) should be restricted. Go to user directory, find all shell configuration scripts, and run these commands:

```
# chown root:root <shell script file>
# chmod 755 <shell script file>
# grep -i umask <shell script file> [and remove the entry if found]
```

Note: Some shell scripts can implicitly call other script files. If so, you must also restrict all dependencies.

For example oracle is a bash user:

```
oracle@berna-vm2:/export/oracle > grep oracle /etc/passwd oracle:x:103:103::/
export/oracle:/bin/bash
oracle@berna-vm2:/export/oracle > cat .bash_profile if [ -f ~/.bashrc ]; then
                  . ~/.bashrc fi

if [ -f ~/.oraUser_profile ]; then
                  . ~/.oraUser_profile fi
…
```

2.9.7 RPC Service disabled to secure passwords

Description **[Full]** RPC service has a vulnerability in providing information. `bootparamd` is used by disk-less clients to obtain boot information. If an attacker uses `BOOTPARAMPROC_WHOAMI` and provides the exact address of the client, then it will have the server's NIS domain. Once the attacker discovers the domain name NIS, can easily obtain the NIS password file. The service should be disabled.

Assess Security Issue

All commands must be run under the super user account:
To check the status of the service:

```
> svcs  -a | grep -i bootparam
```

Fix Security Vulnerability

Disable and stop the service:

```
> svcadm disable svc:/network/rpc/bootparams:default
```

2.9.8 Sensitive files and high-privilege commands limited

Description **[Full]** Permissions granted to the following sensitive files and usage of high privilege commands shall be limited to system administrators. Access to sensitive files for UNIX-based OS, that is, stored password file, network configuration file, and user profile file is limited. Sensitive files for Windows, that is, stored password file; and high privilege commands for all platforms such as start/stop service, generate logs, change system policy, user account management, and network configuration are restricted to administrator access.

Fix Security Vulnerability

The permission, ownership, and group owner setting of these files shall be assigned with these settings:

```
/etc/coreadm.conf                  0544 root:other
/etc/cron.d                        0400 root:root
/etc/cron.d/at.allow               0544 root:sys
/etc/cron.d/at.deny                0544 root:sys
/etc/cron.d/at.deny                0544 root:sys
/etc/cron.d/cron.allow             0544 root:sys


/etc/cron.d/cron.allow             0544 root:sys
/etc/cron.d/cron.deny              0544 root:sys
/etc/default/cron                  0666 root:sys
/etc/default/inetinit              0444 root:sys
/etc/default/keyserv               0444 root:sys
/etc/default/login                 0444 root:sys
/etc/default/passwd                0444 root:sys


/etc/default/power                 0444 root:sys
/etc/default/su                    0444 root:sys
/etc/default/telnetd               0444 root:sys
/etc/default/sys-suspend           0544 root:sys
/etc/ftpd/*                        0544 root:sys
/etc/hosts.allow                   0444 root:root
/etc/hosts.deny                    0444 root:root
```

```
/etc/inet/inetd.conf               0444 root:sys
/etc/init.d/set-tmp-permissions    0555 root:root
/etc/init.d/nddconfig              0555 root:root
/etc/krb5/kdc.conf                 0544 root:root
/etc/mail/sendmail.cf              0444 root:bin
/etc/nscd.conf                     0544 root:sys
/etc/nsswitch.*                    0544 root:sys

/etc/pam.conf                      0544 root:sys
/etc/passwd                        0544 root:sys
/etc/profile                       0544 root:sys
/etc/security/policy.conf          0544 root:sys
/etc/shadow                        0400 root:sys
/etc/shells                        0544 root:sys
/etc/snmp/conf/snmpd.conf          0500 root:sys

/etc/ssh/sshd_config               0544 root:sys
/etc/sudoers                       0440 root:root
/etc/syslog.conf                   0544 root:sys
/etc/system                        0544 root:sys
/etc/user_attr                     0544 root:sys

/usr/bin/truss                     0550 root:bin
/usr/local/etc/sudoers             0440 root:root
/usr/sbin/swap                     0550 root:bin

/var/spool/cron/crontabs           0750 root:bin
/var/spool/cron/crontabs/adm       0600 root:sys
/var/spool/cron/crontabs/root      0600 root:sys
/var/spool/cron/crontabs/sys       0600 root:sys
```

Fix Security Vulnerability

Change the permission, owner, and group owner setting of the previous files using these comands:

```
<hostname>#chmod <permission> <file_name>
<hostname>#chown <user_owner>:<group_owner> <file_name>
```

2.9.9 Security ticket (Kerberos) lifetime less than 600 minutes

Description **[Full]** The maximum Kerberos ticket lifetime shall be set to 600 minutes.

Notes Requires manual reconfiguration because the default parameter is set to `max_life = 8h 0m 0s`.

Assess Security Issue

To check the required parameter value:

```
> grep max_life /etc/krb5/kdc.conf
```

Fix Security Vulnerability

The value of the `max_life` parameter in the `/etc/krb5/kdc.conf` file shall be set to:

```
max_life = 10h 0m 0s
```

To fix the issue, set the required `max_life` value in in the `/etc/krb5/kdc.conf` file.

2.9.10 SSH set higher than version Two

Description **[Full]** Use secure shell (SSH) protocol software version two or later.

Compliance Test

Check the version of SSH in use:

```
> grep Protocol /etc/ssh/sshd_config
```

Required output:

```
Protocol 2
```

Fix Security Vulnerability (Solaris 10)

To fix the issue, set the required protocol version in the `/etc/ssh/sshd_config` file.

Notes

Solaris 11 uses the correct SSH version by default.

2.9.11 Services/protocols, disable insecure and unnecessary ones

Description **[Full]** Disable unnecessary and insecure services and protocols, for example, WWW, FTP, Finger, and Telnet should be disabled.

Notes

All commands must be run under the super user account.
To determine the Solaris version run this command:

```
> uname -r
```

Version 5.10 contains Solaris 10 releases 8/07 and 11/06 mentioned below.

Compliance Test

1. To determine whether the service is active, use this command:

```
> svcs -a | grep -i <service name>
```

(If you have several console lines, just select the necessary service to disable.)

Fix Security Vulnerability (Solaris 10)

Unnecessary services shall be disabled with these commands:

```
> svcadm disable svc:/application/graphical-login/cde-login
> svcadm disable svc:/application/management/snmpdx:default
> svcadm disable svc:/application/management/dmi:default
> svcadm disable svc:/application/management/sma:default
> svcadm disable svc:/application/management/snmpdx:default
> svcadm disable svc:/application/print/rfc1179
> svcadm disable svc:/network/finger:default


> svcadm disable svc:/network/ftp:default
> svcadm disable svc:/network/login:rlogin
> svcadm disable svc:/network/nis/client:default
> svcadm disable svc:/network/nis/passwd:default
> svcadm disable svc:/network/nis/server:default
> svcadm disable svc:/network/nis/update:default
> svcadm disable svc:/network/nis/xfr:default
> svcadm disable svc:/network/rpc/bind
> svcadm disable svc:/network/rpc/bootparams:default
> svcadm disable svc:/network/rpc/cde-calendar-manager
> svcadm disable svc:/network/rpc/cde-ttdbserver:tcp
> svcadm disable svc:/network/rpc/gss
> svcadm disable svc:/network/rpc/nisplus:default
> svcadm disable svc:/network/rpc/smserver:default

> svcadm disable svc:/network/security/ktkt_warn
> svcadm disable svc:/network/tftp/udp6:default
> svcadm disable svc:/network/telnet:default
> svcadm disable svc:/system/filesystem/volfs:default
> svcadm disable svc:/system/webconsole:console
```

[Specific for Solaris 10 which has lower release than 11/06]

```
> /etc/init.d/samba stop
> mv /etc/sfw/smb.conf /etc/sfw/smb.conf.bak
```

[Specific for Solaris 10 which has higher release than 8/07]

```
> svcadm disable svc:/network/samba
```

To stop Apache first run this command:

```
> svcs  -a | grep -i apache
legacy_run      4:20:18 lrc:/etc/rc3_d/S50apache
disabled        4:19:52 svc:/network/http:apache2
```

If the last entry shows `enabled`, run this command:

```
> svcadm disable svc:/network/http:apache2
```

Otherwise check if the following script is available:

```
> ls /etc/rc3.d/S50apache:
```

Otherwise, run these commands:

```
    > /etc/rc3.d/S50apache stop
> mv /etc/rc3.d/S50apache /etc/rc3.d/NoS50apach
```

Fix Security Vulnerability (Solaris 11)

Unnecessary services shall be disabled with these commands:

```
> svcadm disable svc:/network/telnet:default
> svcadm disable svc:/network/ftp:default
> svcadm disable svc:/network/tftp:default
> svcadm disable svc:/application/management/net-snmp:default
> svcadm disable svc:/network/finger:default
> svcadm disable svc:/network/rpc/bind
> svcadm disable svc:/system/webconsole:console

> svcadm disable svc:/application/print/rfc1179
> svcadm disable svc:/network/security/ktkt_warn
> svcadm disable svc:/system/filesystem/volfs:default
> svcadm disable svc:/network/rpc/smserver:default
> svcadm disable svc:/network/rpc/gss
> svcadm disable svc:/network/rpc/nisplus:default
> svcadm disable svc:/network/nis/client:default

> svcadm disable svc:/network/nis/server:default
> svcadm disable svc:/network/nis/passwd:default
> svcadm disable svc:/network/nis/update:default
> svcadm disable svc:/network/nis/xfr:default
> svcadm disable /network/rpc/bootparams:default
> svcadm disable /network/login:rlogin
```

2.9.12 System access .rhosts, .shosts, and .netrc files restricted to administration staff

Description **[Full]** Using `.rhosts`, `.shosts.` and `.netrc` files should be limited only to system administration users. The trusted host and user shall be limited properly based upon need-to-do basis, in `.rhosts` or `/etc/hosts.equiv` files. These files are a major security problem. Protect the files from editing by any non-`root` user.

Assess Security Issue

All commands must be run under the super user account.
Find `.rhosts`, `.shosts`, `.netrc` and `hosts.equiv` files with these commands:

```
> find / -name .rhosts
> find / -name .shosts
> find / -name .netrc
> ls -la /etc/hosts.equiv
```

Fix Security Vulnerability

1. If you find the files in a user home directory (included `root`), remove the files using these commands:

```
> cd <USER_HOME>
> rm .rhosts
> rm .shosts
> rm .netrc
```

2. Create empty `.rhosts`, `.shosts`, `.netrc` files with super user privilege and prohibit write permission for others with these commands:

```
> cd <USER_HOME>
> touch .rhosts
> touch .shosts
> touch .netrc

> chmod 000 .rhosts
> chmod 000 .shosts
> chmod 000 .netrc

> chown root:root .rhosts
> chown root:root .shosts
> chown root:root .netrc
```

3. Remove `/etc/hosts.equiv` or at least limit trusted hosts and user in `/etc/hosts.equiv` files based upon need-to-do basis as in this example:

```
Hostname1 User1
Hostname2 User2
```

Notes

The special character “**+**” as a wild card is strongly prohibited. It provides access from all hosts or for all users without prompting for a password.

2.9.13 XDMCP service disabled

Description **[Full]** XDMCP is inherently insecure. If you must use XDMCP, be sure to use it only in a trusted networks, such as corporate network within a firewall. Never use it in the open network (or Internet) environment without firewall protection. Also, consider using alternative features, such as Nomachine NX, which is a secure version of X. You should disable the XDMCP service running on the server.

Assess Security Issue

All commands must be run under the super user account.
Check the status of the services by running this command:

```
> svcs -a | grep -i cde-login
```

Fix Security Vulnerability

Disable and stop the service using this command:

```
> svcadm disable svc:/application/graphical-login/cde-login:default
```

Index