4. Multilevel Security

This section contains the following information:

- Information on the nature of the UNICOS multilevel security (MLS) system
- Enhancements in the UNICOS MLS 9.0 release
- UNICOS MLS compatibility issues involved in upgrading from the UNICOS MLS 8.0 system to the UNICOS MLS 9.0 system and early information about system changes planned for future UNICOS releases

Because this release overview documents all features and compatibility issues introduced since the UNICOS 8.0 base release, each feature and compatibility issue includes the UNICOS release level in which the feature or compatibility issue was introduced. This information is provided to help our customers focus on the features and compatibility issues that are new specifically for their upgrade.

Each subsection in this section lists in the margin both the type of user and type of hardware affected.

For definitions of the terms used, see subsection 1.6, page 1–6.

4.1 Change in the definition of Trusted UNICOS

The Trusted UNICOS system is a configuration of the UNICOS multilevel security (MLS) system that supports processing at multiple security labels and system administration using only non-super user administrative roles. The Trusted UNICOS system consists of the subset of UNICOS software that offers these capabilities. The Trusted UNICOS name does not imply maintenance of the UNICOS 8.0.2 security rating.

For more information about Trusted UNICOS support in the UNICOS 10.0 release, see subsection 4.3.4.3, page 4–14.

4.2 MLS software enhancements

The following subsections describe enhancements to the UNICOS multilevel security (MLS) system.

For information about UNICOS MLS compatibility issues, see subsection 4.3, page 4–9.

4.2.1 *New functionality for* `ia_user` *library routine*

Users affected

Programmer

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The `ia_user`(3) library routine has been enhanced to support identification only. This extension for `ia_user` allows the caller to ask only for identification service and to specify the type of returned user database (UDB) entry (public or private) directly.

The `IA_IDENTIFICATION` and `IA_PUBLICIDENT` flags were added. The `IA_PUBLICIDENT` flag returns the public UDB entry to the caller. The `IA_IDENTIFICATION` flag tries to return the private UDB entry to the caller, but if the user is not privileged, the public UDB entry is returned and `IA_PUBLIC` error code is returned to warn the caller.

For more information, see the `ia_user`(3) man page.

4.2.2 *MAC read policy restricts pipes*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The mandatory access control (MAC) read policy has been enforced for reading all objects, including pipes. Because reading a pipe is destructive, the act of reading a pipe is actually a write operation. Therefore, pipes can be used to subvert the MAC policy, which is a covert channel.

To close this covert channel, the `Enforce restricted pipes?` selection on the `MLS Systems Option` menu has been added to the UNICOS Installation/Configuration Menu System. This configuration parameter is set to `OFF` by default. Enabling this parameter enforces the new policy that requires a process to have MAC write access to perform a read on a pipe. Also, `getsysv`(2) returns the actual setting of the new parameter.

For more information, see the getsysv(2) and open(2) man pages.

> **Note:** The *UNICOS 8.3 Release Letter* stated that the default setting for the Enforce restricted pipes? configuration selection option would be changed from OFF to ON for UNICOS 10.0 Trusted UNICOS configuration. This change will not be implemented; the Enforce restricted pipes? configuration selection option will still be available and the default setting will remain OFF in the UNICOS 10.0 release.
>
> For more information about Trusted UNICOS support in the UNICOS 10.0 release, see subsection 4.3.4.3, page 4–14.

Related publications

- *General UNICOS System Administration*, publication SG–2301

4.2.3 pathname *routine added*

Users affected

Programmer

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The new pathname(3) library routine provides flexible path resolution and symbolic link expansion to user level programs. This routine understands the semantics of symbolic and multilevel symbolic links, as well as the traditional dot (.) and dot dot (..) directory entries, and it produces true paths from paths that contain these elements.

4.2.4 FSETID_RESTRICT *configuration option changed*

Users affected

Programmer

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The getsysv(2) system call can place the state of the FSETID_RESTRICT configuration parameter in a reserved bit of the sysv structure. This allows applications to use the getsysv system call to determine the state of FSETID_RESTRICT and, if necessary, to manage their behavior accordingly. The value of the sy_fsetid_restrict field in the sysv structure is nonzero if the FSETID_RESTRICT parameter is enabled.

For more information, see the getsysv(2) man page.

4.2.5 SLG_TRUST *record changed*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

Execution of the fsoffload(8), mailx(1), and mail(1) commands generates a trusted process activity record, SLG_TRUST, provided that generation of the SLG_TRUST record type is enabled. UNICOS trusted processes issue the SLG_TRUST record to describe a trusted activity that is performed on behalf of a user. Issuing a trusted process activity record allows a UNICOS trusted process to disable kernel level auditing of its activities and thus reduces the number of audit records that are written.

The changes to mail and mailx reduce the number of audit records generated when a user logs into the system because kernel-level audit records are no longer generated when the mail programs search their directories for new and existing mail messages.

Related publications

- *General UNICOS System Administration*, publication SG–2301

4.2.6 *Security log daemon changed*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The security log daemon, /etc/slogdemon, no longer exits during system initialization if auditing has been disabled. This change improves system resiliency by keeping the daemon available in case the administrator does not enable auditing until after the system has been brought up to multiuser mode.

4.2.7 *MLS support for CRAY T3D systems added*

Users affected

All

Supporting hardware

CRAY T3D systems

Initial release: UNICOS 8.0.4/8.3

Modifications have been made to support the use of a CRAY T3D system on a UNICOS multilevel security (MLS) system with `PRIV_SU` enabled or on a Trusted UNICOS configuration. These UNICOS releases contain the new `/etc/privdb/mpp.db` stub file. The effective version of the `mpp.db` file is installed by the UNICOS MAX operating system.

For information about using the CRAY T3D system in a trusted environment, including levels of the UNICOS MAX system required, refer to the UNICOS MAX 1.2 (or later) release information.

Related publications

- *UNICOS System Security Overview for Administrators*, publication SG–2141

4.2.8 *UNIX System V IPC MLS supported*

Users affected

All

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The UNIX System V interprocess communication (IPC) mechanism introduces three new named object types to the UNICOS multilevel security (MLS) system: shared memory segments (CRAY T90 series only), semaphores, and message queues. These new objects have associated mandatory access control (MAC) label information and access control list (ACL) information that users must be able to set and get by using the user-level commands. The `-M`, `-Q`, `-S`, and `-K` options have been added to the `spset`(1), `spget`(1), and `spclr`(1) commands to allow this information to be set and displayed.

In addition, changes to the `SLG_DISC_7` and `SLG_MAND_7` audit record types allows IPC object creation and use to be audited on a UNICOS MLS system.

For more information, see the spset(1) man page (which documents the spset and spget commands) and the spclr(1) man page.

Related publications

- *General UNICOS System Administration*, publication SG–2301

4.2.9 *New utilities added to the trusted computing base (TCB)*

Users affected

All

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The following utilities have new entries defined in the file /etc/privdb/mls.db of the TCB:

- addbss(1)
- asa(1)
- cksum(1)
- comm(1)
- csplit(1)
- dd(1)
- deplib(1)
- diff3(1)
- fold(1)
- ipcrm(1)
- ipcs(1)
- join(1)
- line(1)
- nasa(1)
- newgrp(1)
- nl(1)
- paste(1)
- renice(1)
- sdiff(1)
- seterr(8)
- setf(1)
- size(1)
- split(1)

- `strings`(1)
- `strip`(1)
- `sum`(1)
- `tsort`(1)

The entry for each utility defines the mandatory access control (MAC) attributes and privilege assignment list (PAL) attributes. The addition of these entries allows these utilities to be used on a Trusted UNICOS system.

For more information, see the man pages for these utilities.

4.2.10 `privcmd` *command enhanced*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

The `privcmd`(8) command no longer requires that security attribute entries for a file be in a specific order. Now, entries for all security attributes can be listed in any order. Also, when making the privilege assignment list (PAL) entry, if two categories are assigned an identical set of privileges and the same privilege text, only a single PAL entry is needed to describe both categories.

The `privcmd`(8) databases created with this new format cannot be processed by versions of `/etc/privcmd` prior to UNICOS 9.0.

Also, the `privcmd`(8) command supplied with UNICOS 8.0 applies all security attributes from the privilege database in the directory `/etc/privdb`. This meant that certain configurations could not be supported. For example, if a site wanted to run a UNICOS multilevel security (MLS) system with `PRIV_SU` and `SECURE_MAC` enabled, `privcmd` did not allow the site to apply the appropriate security labels without also applying discretionary access controls (DACs) and privilege assignment lists (PALs), which were not appropriate for that configuration.

To eliminate this problem, `privcmd`(8) has been enhanced in UNICOS 9.0 to allow a site to specify which grammar object or objects it wants to apply from the privilege database.

The `–S` option and the `grammar_object` operand have been added to `privcmd`(8) to support this new functionality.

For more information, see the `privcmd`(8) man page.

4.2.11 *New MLS field added to the user database (UDB)*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

On the UNICOS 8.0 multilevel security (MLS) system, an administrator could not define a minimum compartment set, although setting the `deflbl_as_minlbl` field of the configuration file forced the compartment set of the user's default security label to serve as the minimum compartment set. (The user's default security label is defined in the user database (UDB).)

The `mincomps` field has been added to the UDB. This field allows a site to define a minimum compartment set for the users. The `deflbl_as_minlbl` field can still be used on UNICOS 9.0 MLS systems to force the user's default security label to be used as the user's minimum security label.

For more information, see the `udbgen`(8) and `libudb`(3) man pages.

For complete information about UDB enhancements in the UNICOS 9.0 release, see subsection 2.9.5, page 2–53.

Related publications

- *UNICOS Multilevel Security (MLS) Feature User's Guide*, publication SG–2111
- *General UNICOS System Administration*, publication SG–2301

4.2.12 *Trusted tape access with Cray/REELlibrarian changed*

Users affected

Administrator

Supporting hardware

All Cray Research systems

Initial release: UNICOS 8.3

On a Trusted UNICOS 8.0 system, a site had to use the Cray/REELlibrarian (CRL) product in order to use tapes.

Trusted UNICOS systems no longer need to have (CRL) to run tapes, if the site permits tape access to administrators only. This new functionality affects only the Trusted UNICOS configurations that are not configured with CRL. Trusted UNICOS systems configured with CRL will continue to work as they did for the UNICOS 8.0 release.

To support this functionality, changes have been made to the UNICOS Installation/Configuration Menu System so that CRL is not automatically required for use on Trusted UNICOS systems. Specifically, the default setting for the tape subsystem option `Enable Cray Reel Librarian (CRL)` is now `NO`. In addition, changes have been made to the privilege assignment list (PAL) of the `rsv`(1) command so that the privileges needed to run this command are assigned to security administrators only.

For more information, see the `rsv`(1) man page.

Related publications

- *UNICOS System Security Overview for Administrators*, publication SG–2141
- *General UNICOS System Administration*, publication SG–2301

4.3 MLS compatibility issues

The following subsections describe user and system administration issues involved in upgrading from the UNICOS 8.0 multilevel security (MLS) system to the UNICOS 9.0 MLS system. This section also includes early information about MLS system changes planned for future UNICOS releases.

4.3.1 *Support for the* `-u` *option of the* `pr` *command dropped*

Users affected

All

Supporting hardware

All Cray Research systems

Incompatibility introduced with release: UNICOS 8.3

Support for the `-u` option of the `pr`(1) command has been dropped as of the UNICOS 9.0 release.

The functionality of the `-u` option was made the default behavior of the `pr`(1) command in the UNICOS 8.0 release, but the `-u` option was retained. In UNICOS 9.0, the option has been dropped completely.

4.3.2 *NQX not supported on UNICOS MLS/Trusted UNICOS systems*

Users affected

All

Supporting hardware

All Cray Research systems

Incompatibility introduced with release: UNICOS 8.0.3/8.3

Unlike the UNICOS 8.0 Network Queuing System (NQS), the Network Queuing EXtensions (NQX) product has not been integrated into the UNICOS multilevel security (MLS) environment and is not part of the trusted computing base of the Trusted UNICOS system. (However, MLS-related NQX problems will be accepted as design SPRs.)

The Network Queuing Environment (NQE) client access to the request status information in the load balancer is controlled by load balancer access control lists (ACLs) instead of security labels. The NQX access from workstations is similar to Remote Queuing System (RQS) or public domain NQS access to the UNICOS MLS system. In these cases, the UNICOS network access list (NAL) controls the label of these connections.

For more information about configuring and using NQX in a UNICOS MLS environment, contact your Cray Research support representative.

4.3.3 *Cray Research publication SN–2133 no longer supported*

Users affected

Administrator

Supporting hardware

All Cray Research systems

As of the UNICOS 9.0 release, the *UNICOS Trusted Network Interface Specification (UTNIS)*, publication SN–2133, is no longer supported.

4.3.4 *Future direction of UNICOS multilevel security (MLS)*

Users affected

All

Supporting hardware

All Cray Research systems

Cray Research has a continuing commitment to support consistent security policies for the UNICOS system. To do this, several features will be incorporated into the UNICOS system during the UNICOS 9.*x* releases, and will be generally available by the UNICOS 10.0 release.

All sites need to be aware of the impact of these upcoming features, especially as they relate to migration and compatibility issues. For sites that are currently using a UNICOS non-MLS system, the UNICOS 10.0 system will have the same behavior as the current UNICOS system used by your site. For sites that are currently using a UNICOS MLS system, your site may have migration and/or compatibility issues, depending on the UNICOS MLS configuration you are using currently. The features are as follows:

- Merge the UNICOS non-MLS and MLS systems
- Remove support for the UNICOS 7.0 trusted system management (TFMgmt) mechanism (`PRIV_TFM`)
- Remove the Trusted UNICOS configuration option
- Support only the following system management mechanisms to enforce the assigning of privileges:
  - a `PRIV_SU` system with privilege assignment lists (PALs)
  - a non-`PRIV_SU` system with PALs
- Change the default setting of the `FSETID_RESTRICT` configuration parameter
- Reduce the number of security-related configuration parameters

Each of these features and their associated impacts is discussed in more detail in the following subsections.

4.3.4.1 *UNICOS non-MLS and MLS systems to be merged*

Users affected

End user, administrator

Supporting hardware

All Cray Research systems

On the UNICOS 8.0 and 9.0 systems, the MLS configuration is optional. That is, to use security features specific to the UNICOS MLS configuration, sites must enable the `SECURE_CONFIG` configuration parameter.

As of the UNICOS 10.0 release, the `SECURE_CONFIG` parameter will not be supported, and the MLS features will be incorporated into the UNICOS 10.0 system.

Combining the non-MLS and MLS systems makes the security features, such as access control lists (ACLs) and security auditing, available to all Cray Research customers. Use of these security features will still be optional. Sites can choose to use only those features that are applicable to their sites.

For sites that are currently using a UNICOS non-MLS system, this feature will provide a UNICOS configuration that has the same behavior as the current UNICOS non-MLS system. For sites that are currently using a UNICOS MLS system, this feature will provide a UNICOS configuration that has the same behavior as the current UNICOS MLS system. Commands, libraries, and system calls will not change. However, interfaces that are currently available only on UNICOS MLS systems will be generally available on UNICOS 10.0 systems.

Changes will be made to some of the default settings of options in the UNICOS Installation/Configuration Menu System. These changes will not impact sites that import their previous configurations.

4.3.4.2 `PRIV_TFM` *configuration option to be removed*

Users affected:

Administrator

Supporting hardware:

All Cray Research systems

UNICOS MLS configurations using the UNICOS 7.0 style trusted facility management, TFMgmt, (also referred to as `PRIV_TFM`) were supported in the UNICOS 8.0 release and will be supported in the UNICOS 9.0 release. On a `PRIV_TFM` system, the administrative roles of operator, system administrator, and security administrator are available, but design problems exist. A `PRIV_TFM` system does not support true separation of administrative roles, and when used in a MLS environment (that is, nonzero security labels are used), many system utilities function incorrectly.

Support for UNICOS MLS systems with `PRIV_TFM` enabled will be dropped as of the UNICOS 10.0 release and the `PRIV_TFM` configuration option will no longer be available through the UNICOS Installation/Configuration Menu System. Also, support for the `tsubcmd`(8) and `udbcmd`(8) commands (which are used to install system binaries that require 7.0 TFMgmt security labels), and the associated man pages will be dropped as of the UNICOS 10.0 release. All references to 7.0 TFMgmt and/or `PRIV_TFM` will be removed from the UNICOS 10.0 documentation.

In addition, support for the `SYSTEM_ADMIN_CONSOLE`, `SECURE_SYSTEM_CONSOLE`, and `SECURE_OPERATOR_CONSOLE` configuration parameters will also be dropped as of UNICOS 10.0. The functionality provided by these parameters will no longer be available. References to these parameters will be removed from the UNICOS 10.0 documentation.

System calls and commands that manage PRIV_TFM user classes, file classes, and file categories will continue to be available in the UNICOS 10.0 release. However, setting user class, file class, and file category attributes will serve no useful purpose, because the UNICOS system will no longer use those attributes to make security-related decisions.

All PRIV_TFM interfaces will be removed in a future UNICOS release. During the UNICOS 9.0 release, to prepare for the removal of PRIV_TFM interfaces, you should perform the following steps:

- Use of the setucls(2), setcls(2), setfcat(2), and settfm(2) system calls should be eliminated from applications.
- Use of the setucls(1) and the -i and -j options of the spset(1) commands should be eliminated from shell scripts.
- Use of the setfflg(2) to set the TFM_EXEC file flag should be eliminated from applications.
- Use of the -k option of the spset(1) command to set the exec file flag should be eliminated from shell scripts.
- Values in the st_intcls and st_intcat fields of the secstat structure should not be used to make decisions. The st_secflg field of the secstat structure should not be checked for the exec flag value.
- Values in the sv_intcls and sv_intcat fields of the usrv structure should not be used to make decisions.
- Applications should not depend on the output format of the spget(1) command with no options supplied. Display of the user class information will be eliminated.
- Applications should not depend on the output format of the spget(1) command with the –f option supplied. Display of the file class, file category, and the 'exec' file flag will be eliminated.
- Applications should not depend on the output format of the ls(1) command with the -e option supplied. Display of the i field, which indicates a nonzero file category or class, will be eliminated.
- Applications should not depend on the output format of all other commands that display user class, file class, or file category information. Those commands include udbsee(1), crash(8), reduce(8), and so on.

4.3.4.3 *Trusted UNICOS configuration option to be removed*

Users affected:

Administrator

Supporting hardware:

All Cray Research systems

The Trusted UNICOS configuration was first introduced in the UNICOS 8.0 release. The National Security Agency (NSA) evaluated this configuration and gave it a B1 MDIA[†] rating in March 1994. Support for the Trusted UNICOS configuration continues in the UNICOS 9.0 release, although no evaluation was done. Cray Research has no plans for a future evaluation.

As of the UNICOS 10.0 release, the functionality of the Trusted UNICOS system will be retained, but the `CONFIG_TRUSTED` option, which enforces conformance to the strict B1 configuration, will no longer be available. All references to Trusted UNICOS systems will be removed from the UNICOS 10.0 documentation.

[†] B1 is a class defined in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC). This class represents a set of security criteria for computer systems. MDIA is an acronym defined in the Trusted Network Interpretation (TNI). It is formed by combining the first letter of the following four security policies, which network components can support in order to obtain an evaluated rating:

M=Mandatory access control (MAC)
D=Discretionary access control (DAC)
I=Identification and authentication (I&A)
A=Audit

4.3.4.4 *Supported system management configurations in UNICOS 10.0*

Users affected:

Administrator

Supporting hardware:

All Cray Research systems

On UNICOS 9.0 MLS systems, the ability to define different administrative tasks and roles is called trusted facility management. For the UNICOS 10.0 MLS release, this concept will be replaced with the term “system management.” *System management* addresses the security-related aspects of system administration, operation, and maintenance. It provides administrative and operational policies and procedures for maintaining system security.

On a UNICOS 10.0 MLS system, system management will support the option of the all-powerful root administrative role. It will also support the definition of roles by assigning each role an administrative category. For example, the security administrator role is assigned the `secadm` category, while the operator role is assigned the `sysops` category. Categories are used in conjunction with the UNICOS privilege assignment list (PAL) -based privilege mechanism to assign different administrative tasks to each administrative role.

The UNICOS 10.0 MLS system will support the following mechanisms to enforce the assigning of privileges:

- A super user (`PRIV_SU`) system with PALs
- A non-super user (non-`PRIV_SU`) system with PALs

The use of a super user on a UNICOS MLS system (enabled by using the `PRIV_SU` configuration option) was introduced in the UNICOS 8.0 release and granted a root user full administrator control.

PALs were introduced in the UNICOS 8.0 release and were used to separate administrative roles. The PALs were applied only when the `privcmd`(8) command was executed. The use of PALs and the way they are applied continues in the UNICOS 9.0 system. Only a subset of the UNICOS software is supported by PALs in the UNICOS 8.0 and UNICOS 9.0 releases. This subset of software is basically the set of software defined for the Trusted UNICOS 8.0 and UNICOS 9.0 systems. As of the UNICOS 10.0 release, PALs will be applied on all systems and will continue to support only a subset of UNICOS software.

Sites must decide which UNICOS 10.0 system management configuration they want to use. Sites that do not need the strict separation of administrative roles will probably want to use the PRIV_SU system with PALs. Sites needing stricter security measures will probably want to use the non-PRIV_SU system with PALs.

Regardless of which system management configuration is used, PALs must be assigned on all UNICOS 10.0 systems. Once these PALs are assigned, their effect will be transparent on systems administered only by the root user. The PRIV_SU system without PALs that is supported in the UNICOS 8.0 and UNICOS 9.0 releases will not be supported in the UNICOS 10.0 release.

4.3.4.5 *Reduction of security-related configuration options*

Users affected:

End user, administrator

Supporting hardware:

All Cray Research systems

The number of configuration options related to security will be reduced in the UNICOS 10.0 release.

The configuration options that will be deleted are as follows:

- MAC_COMMAND
- MLS_INTEGRITY
- PRIV_TFM
- SECURE_MLSDIR
- SECURE_MOUNT
- SECURE_REMOTE
- STAT_RESTRICT

Removal of these configuration options could cause migration issues for sites upgrading from a UNICOS 9.0 MLS system to a UNICOS 10.0 system. All UNICOS 10.0 documentation will be updated to reflect the removal of these options.

The following list describes the impact of removing these configuration options. Where appropriate, restrictions can be bypassed by an authorized administrator.

Option	Impact
`MAC_COMMAND`	When this option is removed, subjects will be permitted to view information for an object only when the subject dominates the object, which is consistent with the current MLS mandatory access control (MAC) policy.
`MLS_INTEGRITY`	This UNICOS MLS option is not currently used.
`PRIV_TFM`	See subsection 4.3.4.2, page 4–12, for more information.
`SECURE_MLSDIR`	When this option is removed, a user with a label that dominates but does not equal the label of the parent directory will no longer be allowed to create a subdirectory in that parent directory. Instead, a user at the label of the parent directory will be allowed to create a subdirectory with a higher label, or upgrade an existing subdirectory provided that the subdirectory is empty and is initially at the same label as the user.
`SECURE_MOUNT`	This option becomes obsolete as of the UNICOS 10.0 release because of the merging of UNICOS non-MLS and MLS systems (see subsection 4.3.4.1, page 4–11). All file systems (including UNICOS non-MLS file systems) will be treated as labeled file systems.
`SECURE_REMOTE`	This UNICOS MLS option is not currently used.
`STAT_RESTRICT`	When this option is removed, a subject will be able to perform a `stat`(2) operation only for an object that the subject dominates, which is consistent with the current MLS MAC policy.

4.3.4.6 *Default value of the* FSETID_RESTRICT *configuration parameter to be changed*

Users affected:

Administrator

Supporting hardware:

All Cray Research systems

Beginning with the UNICOS 10.0 release, the default value of the FSETID_RESTRICT configuration parameter will be OFF. This will be a change from the default value on UNICOS 9.0 MLS systems, which is ON.

4.3.4.7 *MLS documentation changes*

Users affected:

All

Supporting hardware:

All Cray Research systems

Because of the features outlined previously, the relevant sections of the *UNICOS Multilevel Security (MLS) Feature User's Guide*, publication SG–2111, and the *UNICOS System Security Overview for Administrators*, publication SG–2141, will be merged into other UNICOS man pages, user manuals, and administrator manuals. You will not be able to order these two publications for the UNICOS 10.0 release.

4.3.5 *Changes to* su *password use for system administrators*

Users affected:

Administrator

Supporting hardware:

All Cray Research systems

In an upcoming UNICOS 9.0 bugfix release, a user with an active sysadm category can no longer use the su(1) command without supplying a password. This change affects sites using UNICOS MLS systems with privilege assignment lists (PALs). The supported PAL for /bin/su was updated to remove the sysadm PAL category record. In addition, the su(1) man page was updated to reflect this change.

This change was introduced to prevent users with a sysadm category from gaining other types of administrative capabilities by invoking the su command without a password to assume the identity of another administrator, and subsequently using facilities that perform reauthentication using that new user ID.

Sites that do not approve of the new restriction, and that are willing to assume the risks of preserving the previous functionality, can add the original /bin/su PAL definition to the /etc/config/localpriv.db file.