(Solaris for Intel Section about the Sha256 and Sha512 patch, updated patch)

http://sunsolve.sun.com/search/document.do?assetkey=1-21-140906-02-1

SunOS 5.10_x86: sha256, sha512 patch

Status: RELEASED

Patch Id: 140906-02

****

READ THE TERMS OF THE AGREEMENT ("AGREEMENT") IN THE LEGAL_LICENSE.TXT

FILE CAREFULLY BEFORE USING THIS SOFTWARE. BY USING THE SOFTWARE, YOU

AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE

TERMS, PROMPTLY DESTROY THE UNUSED SOFTWARE.

****

For further information on patching best practices and resources, please

see the Big Admin Patching Center, http://www.sun.com/bigadmin/patches/

****

Summary: SunOS 5.10_x86: sha256, sha512 patch

Date: May/28/2010

Installation Requirements:

Reboot after installing this patch to activate the changes delivered. An alternative may be specified in the Special Install Instructions.

Solaris Release: 10_x86

Sun OS Release: 5.10_x86

Unbundled Product:

Unbundled Release:

Xref: This patch available for SPARC as patch 140905

Topic:

SunOS 5.10_x86: sha256, sha512 patch

Relevant Architecture: i386

BugId's fixed with this patch:

6733782 6836636

Changes incorporated in this version:

6836636

Patches accumulated and obsoleted by this patch:

140858-01

Patches which conflict with this patch:

Required Patches:

137138-09 (or greater)

Obsoleted by:

Files Included in this Patch:

/usr/lib/security/amd64/crypt_sha256.so.1

/usr/lib/security/amd64/crypt_sha512.so.1

/usr/lib/security/crypt_sha256.so.1

/usr/lib/security/crypt_sha512.so.1

Problem Description:

6836636 crypt_sha256 and crypt_sha512 modules ignore rounds setting in crypt.conf

(from 140906-01)

```
        This revision accumulates generic Sustaining patch 140858-01

        into Solaris S10U7 update.
```

(from 140858-01)

6733782 sha256 algorithm incorrectly builds final salt string

Revision History:

140906-01 140858-01

Patch Installation Instructions:

Please refer to the man pages for instructions on using 'patchadd'
and 'patchrm' commands provided with Solaris.

The following example installs a patch to a standalone machine:

```
       example# patchadd /var/spool/patch/123456-07
```

The following example removes a patch from a standalone system:

```
       example# patchrm 123456-07
```

For additional examples please see the appropriate man pages. Any
other special or non-generic installation instructions should be
described below as special instructions.

Special Install Instructions:

None.

README -- Last modified date: Friday, May 28, 2010

(Solaris for Sparc Section about the Sha256 and Sha512 patch, updated patch)

http://sunsolve.sun.com/search/document.do?assetkey=1-21-140905-02-1

Status: RELEASED
Patch Id: 140905-02
****
READ THE TERMS OF THE AGREEMENT ("AGREEMENT") IN THE LEGAL_LICENSE.TXT FILE CAREFULLY BEFORE USING THIS SOFTWARE. BY USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS, PROMPTLY DESTROY THE UNUSED SOFTWARE.
****
For further information on patching best practices and resources, please see the Big Admin Patching Center, http://www.sun.com/bigadmin/patches/
****
Summary: SunOS 5.10: sha256, sha512 patch
Date: May/21/2010
Installation Requirements:
Reboot after installing this patch to activate the changes delivered. An alternative may be specified in the Special Install Instructions.
Solaris Release: 10
Sun OS Release: 5.10
Unbundled Product:
Unbundled Release:
Xref: This patch available for x86 as patch 140906
Topic:
SunOS 5.10: sha256, sha512 patch
Relevant Architecture: sparc
BugId's fixed with this patch:

6733782 6836636

Changes incorporated in this version:

6836636

Patches accumulated and obsoleted by this patch:

140857-01

Patches which conflict with this patch:
Required Patches:

137137-09 (or greater)

Obsoleted by:

Files Included in this Patch:
/usr/lib/security/crypt_sha256.so.1
/usr/lib/security/crypt_sha512.so.1
/usr/lib/security/sparcv9/crypt_sha256.so.1
/usr/lib/security/sparcv9/crypt_sha512.so.1

Problem Description:
6836636 crypt_sha256 and crypt_sha512 modules ignore rounds setting in crypt.conf

(from 140905-01)

        This revision accumulates generic Sustaining patch 140857-01
        into Solaris S10U7 update.

(from 140857-01)

6733782 sha256 algorithm incorrectly builds final salt string
Revision History:

140857-01 140905-01

Patch Installation Instructions:

Please refer to the man pages for instructions on using 'patchadd' and 'patchrm' commands provided with Solaris.

The following example installs a patch to a standalone machine:

```
       example# patchadd /var/spool/patch/123456-07
```

The following example removes a patch from a standalone system:

```
       example# patchrm 123456-07
```

For additional examples please see the appropriate man pages. Any other special or non-generic installation instructions should be described below as special instructions.
Special Install Instructions:

None.

README -- Last modified date: Friday, May 21, 2010