

# SSRT3613 rev.1 HP-UX B6848AB GTK+ Support Libraries elevated privileges

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.sys.hp.hpux/2005-02/0249.html>

---

*From:* Security Alert (*secure\_at\_hpchs.cup.hp.com*)

*Date:* 02/24/05

Date: Thu, 24 Feb 2005 12:43:49 GMT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

HP SECURITY BULLETIN

HPSBUX01034 REVISION: 1

SSRT3613 rev.1 HP-UX B6848AB GTK+ Support Libraries  
elevated privileges

NOTICE:

There are no restrictions for distribution of this Security Bulletin provided that it remains complete and intact.

The information in this Security Bulletin should be acted upon as soon as possible.

INITIAL RELEASE:

22 February 2005

POTENTIAL SECURITY IMPACT:

elevated privileges for a local authorized user.

SOURCE:

Hewlett-Packard Company

HP Software Security Response Team

VULNERABILITY SUMMARY:

A potential vulnerability has been identified with HP-UX running B6848AB GTK+ Support Libraries where a directory permissions issue could be exploited to allow a local authorized user to gain elevated privileges.

REFERENCES:

None

comp.sys.hp.hpux: SSRT3613 rev.1 HP-UX B6848AB GTK+ Support Libraries elevated privileges

SUPPORTED SOFTWARE VERSIONS\*: ONLY impacted versions are listed.  
HP-UX B.11.00, B.11.11 with B6848AB GTK+ Support Libraries  
installed

BACKGROUND:

The product B6848AB (GTK+ Libraries) is available for  
download from software.hp.com:

<[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/  
displayProductInfo.pl?productNumber=B6848AB](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6848AB)>

The source files in this product are world writable.  
After the product is installed any user can modify the  
source. If new libraries are to be built using this  
source code the files should be verified.

The web page above has the following description of B6848AB:

The GTK+ Libraries are the open source GNU toolkit for X  
windows development. The version provided here is  
unsupported, but is provided for use with the unsupported  
Mozilla browser for 10.20 and for old versions of Netscape  
(i.e. 6.2.1), which depend on it. We recommend upgrading to  
a newer browser/OS combo, such as Mozilla for HP-UX 11.0  
and later, which require a newer version of the GTK.

Note: Product B6848BA (ximian gnome 1.4 gtk+ libraries for  
hp-ux) does NOT have this permissions problem.

AFFECTED VERSIONS

Note: To determine if a system has an affected version,  
search the output of "swlist -a revision -l fileset"  
for an affected fileset. Then determine if the  
recommended patch or update is installed.

HP-UX B.11.00

HP-UX B.11.11

=====

GTK+.GTK+-SRC

GLib.GLIB-SRC

-> action: install revision 1.2.10.2.1 or subsequent.

Gettext.GETTEXT-SRC

-> action: install revision 0.10.39.2.1 or subsequent.

END AFFECTED VERSIONS

RESOLUTION:

An updated version of B6848BA which corrects the file  
permissions is available from <http://software.hp.com>.

Note: The directory permissions are secure in all versions of B6848BA. However, only versions of B6848BA  
-> containing the following file sets resolve the  
-> permissions issue for directories installed by B6848AB:

-> GTK+.GTK+-SRC, revision 1.2.10.2.1 or subsequent.  
-> GLib.GLIB-SRC, revision 1.2.10.2.1 or subsequent.  
-> Gettext.GETTEXT-SRC, revision 0.10.39.2.1 or  
-> subsequent.

Note: B6848AB is only required for Netscape 6, which is no longer supported on HP-UX. The recommended solution is HP's Mozilla ([www.hp.com/go/mozilla](http://www.hp.com/go/mozilla)), which requires B6848BA.

If the obsolete B6848AB is needed:

1. Remove B6848AB.
2. Reinstall B6848AB.
3. Immediately make the following changes to directory permissions:

```
chmod 555 /opt/gnome/src/GLib/glib-1.2.8
chmod 555 /opt/gnome/src/GLib/glib-1.2.8/docs
chmod 555 /opt/gnome/src/GLib/glib-1.2.8/gmodule
chmod 555 /opt/gnome/src/GLib/glib-1.2.8/gthread
chmod 555 /opt/gnome/src/GLib/glib-1.2.8/tests
chmod 555 /opt/gnome/src/GTK+/gtk+-1.2.10
chmod 555 /opt/gnome/src/GTK+/gtk+-1.2.10/docs
chmod 555 /opt/gnome/src/GTK+/gtk+-1.2.10/gdk
chmod 555 /opt/gnome/src/GTK+/gtk+-1.2.10/gtk
chmod 555 /opt/gnome/src/GTK+/gtk+-1.2.10/po
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/doc
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/intl
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/lib
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/m4
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/misc
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/po
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/src
chmod 555 /opt/gnome/src/Gettext/gettext-0.10.35/tests
```

MANUAL ACTIONS: Yes – Update

If B6848AB is needed:

- >Remove B6848AB.
- >Reinstall B6848AB.
- >Manually change directory permissions.

**BULLETIN REVISION HISTORY:**

Revision 0: 10 May 2004

Initial release

Revision 1: 22 February 2005

Changed action to install B6848BA.

Corrected manual actions.

HP-UX SPECIFIC SECURITY BULLETINS\*: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA)

**SUPPORT:** For further information, contact normal HP Services support channel.

**REPORT:** To report a potential security vulnerability with any HP supported product, send Email to: security-alert@hp.com. It is strongly recommended that security related information being communicated to HP be encrypted using PGP, especially exploit information. To obtain the security-alert PGP key please send an e-mail message to security-alert@hp.com with the Subject of 'get key' (no quotes).

**SUBSCRIBE:** To initiate a subscription to receive future HP Security Bulletins via Email:

[http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in\\_SC-GEN\\_\\_driverITRC&topiccode=ITRC](http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in_SC-GEN__driverITRC&topiccode=ITRC)

On the web page: ITRC security bulletins and patch sign-up

Under Step1: your IRTC security bulletins and patches

- check ALL categories for which alerts are required and continue.

Under Step2: your IRTC operating systems

- verify your operating system selections are checked and save.

To update an existing subscription:

<http://h30046.www3.hp.com/subSignIn.php>

Log in on the web page

Subscriber's choice for Business: sign-in.

On the Web page:

Subscriber's Choice: your profile summary

- use Edit Profile to update appropriate sections.

To review previously published Security Bulletins visit:  
<http://itrc.hp.com/service/cki/secBullArchive.do>

\* The Software Product Category that this Security Bulletin relates to is represented by the 5th and 6th characters of the Bulletin number:

GN = HP General SW,  
MA = HP Management Agents,  
MI = Misc. 3rd party SW,  
MP = HP MPE/iX,  
NS = HP NonStop Servers,  
OV = HP OpenVMS,  
PI = HP Printing & Imaging,  
ST = HP Storage SW,  
TL = HP Trusted Linux,  
TU = HP Tru64 UNIX,  
UX = HP-UX,  
VV = HP Virtual Vault

System management and security procedures must be reviewed frequently to maintain system integrity. HP is continually reviewing and enhancing the security features of software products to provide customers with current secure solutions.

"HP is broadly distributing this Security Bulletin in order to bring to the attention of users of the affected HP products the important security information contained in this Bulletin. HP recommends that all users determine the applicability of this information to their individual situations and take appropriate action. HP does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, HP will not be responsible for any damages resulting from user's use or disregard of the information provided in this Bulletin. To the extent permitted by law, HP disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non-infringement."

(c)Copyright 2005 Hewlett-Packard Development Company, L.P. Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HP nor its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein are trademarks of Hewlett-Packard Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their

comp.sys.hp.hpux: SSRT3613 rev.1 HP-UX B6848AB GTK+ Support Libraries elevated privileges  
respective owners.

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1

iQA/AwUBQhx2+eAfOvwtKn1ZEqJCsgCeNLC4yADoauhXffP3FIHCrD7AD+MAnA3n  
yMi9+ch+d1DwFNG0ku8NxpHA  
=Az5Z

-----END PGP SIGNATURE-----

--

Yours truly,  
HP S/W Security Team  
WTEC Cupertino, California  
Return-Path: secure@cup.hp.com  
Reply-to: security-alert@hp.com