

# Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-04/0379.html>

---

**From:** Security Alert ([secure@cup.hp.com](mailto:secure@cup.hp.com))

**Date:** 04/23/03

From: [secure@cup.hp.com](mailto:secure@cup.hp.com) (Security Alert)

Date: 23 Apr 2003 06:54:29 -0700

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

Hash: SHA1

-----  
\*\*REVISED 02\*\*

Source: HEWLETT-PACKARD COMPANY

SECURITY BULLETIN: HPSBUX0303-252

Originally issued: 19 March 2003

Last revised: 22 April 2003

SSRT2439 Potential Security Vulnerability in xdrmem\_getbytes()  
(rev.2)

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

The information in the following Security Bulletin should be  
acted upon as soon as possible. Hewlett-Packard Company will  
not be liable for any consequences to any customer resulting  
from customer's failure to fully implement instructions in this  
Security Bulletin as soon as possible.

-----  
PROBLEM: Potential buffer overflow in xdrmem\_getbytes() and  
related functions.

IMPACT: Potential unauthorized access, denial of service.

PLATFORM: HP 9000 Series 700 and 800 10.20, 11.00, 11.04, 11.11,  
and 11.22

SOLUTION: Until patches are available manually install the  
appropriate fixed libraries.

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

MANUAL ACTIONS: Yes – NonUpdate

Download and install the appropriate files.

AVAILABILITY: The files are available now. This bulletin will be revised when patches are available.

CHANGE SUMMARY: Rev.01 – Corrected instructions for replacing libc.1 on 11.00 and 11.11.  
Added CERT CA–2003–10 reference.  
Rev.02 – Corrected instructions 10.20

---

## A. Background

There are potential buffer overflows in xdrmem\_getbytes() and related functions.

This issue has been reported by CERT/CC in advisory CA–2003–10.

### NOTE:

The files listed below also have the fix for HPSBUX0209–215  
SSRT2336 Security Vulnerability in XDR library  
This bulletin should be implemented instead of HPSBUX0209–215.

### HP Tru64 UNIX/TruCluster Servers:

The following potential security vulnerability has been identified or reported in the HP Tru64 UNIX operating system that may result in unauthorized Privileged Access or a Denial of Service (DoS).

This potential vulnerability may be in the form of Local and Remote security domain risks.

Cross reference: SSRT2322, SSRT2384, SSRT2341, SSRT2439,SSRT2412

Not Impacted:

HP NonStop Servers  
HP OpenVMS

## B. Recommended solution

Until patches are released, download and manually install the appropriate libraries.

System: hprc.external.hp.com (192.170.19.51)  
Login: xdr2  
Password: xdr2

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

Browser ftp access:

<ftp://xdr2:xdr2@hprc.external.hp.com/>

or

<ftp://xdr2:xdr2@192.170.19.51/>

Note: There is an ftp defect in IE5 that may result in a browser hang. To work around this:  
Select Tools -> Internet Options -> Advanced  
Un-check the option: [ ] Enable folder view for FTP sites

If you wish to verify the md5 sum please refer to:

HPSBUX9408-016  
Patch sums and the MD5 program

Download the appropriate files and unpack with gunzip:

libc.1.gz # 10.20, 11.00, 11.04,  
          # 11.11, 11.22  
libnsl.1.32\_11.00.gz # 11.00, 11.04  
libnsl.a.32\_11.00.gz # 11.00, 11.04  
libnsl.1.64\_11.00.gz # 11.00, 11.04  
libnsl.a.64\_11.00.gz # 11.00, 11.04  
libnsl.1.32\_11.11.gz # 11.11  
libnsl.a.32\_11.11.gz # 11.11  
libnsl.1.64\_11.11.gz # 11.11  
libnsl.a.64\_11.11.gz # 11.11  
libnsl.so.1.32\_11.22IA.gz # 11.22  
libnsl.so.1.64\_11.22IA.gz # 11.22

Verify the cksum or md5.

If you wish to verify the md5 sum please refer to:

HPSBUX9408-016  
Patch sums and the MD5 program

cksum:

3108550729 1867776 libc.1  
2543748420 679936 libnsl.1.32\_11.00  
276323054 724992 libnsl.1.32\_11.11  
3883898582 652664 libnsl.1.64\_11.00  
3213617762 702976 libnsl.1.64\_11.11  
2393869471 818268 libnsl.a.32\_11.00  
247758007 784780 libnsl.a.32\_11.11  
205723668 1456024 libnsl.a.64\_11.00  
113343780 1521756 libnsl.a.64\_11.11  
2149197207 1490400 libnsl.so.1.32\_11.22IA  
755476395 1565336 libnsl.so.1.64\_11.22IA

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

MD5 (libc.1) = 118ce482dbb3982b7484ddc434d77a51  
MD5 (libnsl.1.32\_11.00) = a6bbfcae4a7044b0d1e9aece871c126e  
MD5 (libnsl.1.32\_11.11) = 4bf6edc87dac7a3e5fc23eb4587cbe52  
MD5 (libnsl.1.64\_11.00) = b3c76866d75a4216be7787f219c051df  
MD5 (libnsl.1.64\_11.11) = df6236d0ed6322288cc3d14d788d4b57  
MD5 (libnsl.a.32\_11.00) = 1c0aea725173673eb1c8e9410180096c  
MD5 (libnsl.a.32\_11.11) = 19bf43a94322d0217dfad0a57b19fbac  
MD5 (libnsl.a.64\_11.00) = 06c8fd367c7620a017e9bb2e7df3ec7d  
MD5 (libnsl.a.64\_11.11) = 39dec91e1cff50007ed7abc59bf2515a  
MD5 (libnsl.so.1.32\_11.22IA) = 6da4151346312058269645856e16ac89  
MD5 (libnsl.so.1.64\_11.22IA) = f5f89dd00c66d03d7e14a72232c86f25

For 10.20

=====

Go to init state 2

#DIR=[path to new files]

#cd /usr/lib

#cp libc.1 libc.1.orig

#cp \$DIR/libc.1 libc.1.new

#chown bin libc.1.new

#chgrp bin libc.1.new

\*\*REVISED 02\*\*

--> #chmod 555 libc.1.new

--> #/sbin/mv libc.1 was.libc.1

--> #/sbin/mv libc.1.new libc.1

Reboot the system.

rm /usr/lib/was.libc.1

For 11.00 and 11.04

=====

#DIR=[path to new files]

#cd /usr/lib

#cp \$DIR/libnsl.1.32\_11.00 libnsl.1.new

#cp \$DIR/libnsl.a.32\_11.00 libnsl.a.new

#cp \$DIR/libc.1 libc.1.new

#chmod 555 libnsl.1.new

#chmod 444 libnsl.a.new

#chmod 555 libc.1.new

#chown bin:bin libnsl.1.new

#chown bin:bin libnsl.a.new

#chown bin:bin libc.1.new

#mv libnsl.1 libnsl.1.orig

#mv libnsl.a libnsl.a.orig

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

```
#mv libc.1 libc.1.orig

#mv libnsl.1.new libnsl.1
#mv libnsl.a.new libnsl.a
#mv libc.1.new libc.1

#cd /usr/lib/pa20_64

#cp $DIR/libnsl.1.64_11.00 libnsl.1.new
#cp $DIR/libnsl.a.64_11.00 libnsl.a.new

#chmod 555 libnsl.1.new
#chmod 444 libnsl.a.new

#chown bin:bin libnsl.1.new
#chown bin:bin libnsl.a.new

#mv libnsl.1 libnsl.1.orig
#mv libnsl.a libnsl.a.orig

#mv libnsl.1.new libnsl.1
#mv libnsl.a.new libnsl.a
```

After this, any applications that use libnsl.1 must be restarted. Any applications that use libnsl.a must be relinked and restarted. Any applications that use libc.1 must be restarted.

Rebooting is the recommended way to restart the applications using libnsl.1 or libc.1.

For 11.11 (11i)

```
=====
#DIR=[path to new files]
#cd /usr/lib

#cp $DIR/libnsl.1.32_11.11 libnsl.1.new
#cp $DIR/libnsl.a.32_11.11 libnsl.a.new
#cp $DIR/libc.1 libc.1.new

#chmod 555 libnsl.1.new
#chmod 444 libnsl.a.new
#chmod 555 libc.1.new

#chown bin:bin libnsl.1.new
#chown bin:bin libnsl.a.new
#chown bin:bin libc.1.new

#mv libnsl.1 libnsl.1.orig
#mv libnsl.a libnsl.a.orig
#mv libc.1 libc.1.orig
```

## comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

```
#mv libnsl.1.new libnsl.1
#mv libnsl.a.new libnsl.a
#mv libc.1.new libc.1

#cd /usr/lib/pa20_64

#cp $DIR/libnsl.1.64_11.11 libnsl.1.new
#cp $DIR/libnsl.a.64_11.11 libnsl.a.new

#chmod 555 libnsl.1.new
#chmod 444 libnsl.a.new

#chown bin:bin libnsl.1.new
#chown bin:bin libnsl.a.new

#mv libnsl.1 libnsl.1.orig
#mv libnsl.a libnsl.a.orig

#mv libnsl.1.new libnsl.1
#mv libnsl.a.new libnsl.a
```

After this, any applications that use libnsl.1 must be restarted. Any applications that use libnsl.a must be relinked and restarted.

Rebooting is the recommended way to restart the applications using libnsl.1 or libc.1.

For 11.22 IA

```
=====
#DIR=[path to new files]
#cd /usr/lib/hpux32
#cp $DIR/libnsl.so.1.32_11.22.IA libnsl.so.1.new
#chmod 555 libnsl.so.1.new
#chown bin:bin libnsl.so.1.new
#mv libnsl.so.1 libnsl.so.1.orig
#mv libnsl.so.1.new libnsl.so.1

#cd /usr/lib
#cp $DIR/libc.1 libc.1.new
#chmod 555 libc.1.new
#chown bin:bin libc.1.new
#mv libc.1 libc.1.orig
#mv libc.1.new libc.1

#cd /usr/lib/hpux64
#cp $DIR/libnsl.so.1.64_11.22.IA libnsl.so.1.new
#chmod 555 libnsl.so.1.new
#chown bin:bin libnsl.so.1.new
#mv libnsl.so.1 libnsl.so.1.orig
#mv libnsl.so.1.new libnsl.so.1
```

## comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

After this, any applications that use libnsl.so.1 must be restarted.

Rebooting is the recommended way to restart the applications using libnsl.1 or libc.1.

C. To subscribe to automatically receive future NEW HP Security Bulletins from the HP IT Resource Center via electronic mail, do the following:

Use your browser to get to the HP IT Resource Center page at:

<http://itrc.hp.com>

Use the 'Login' tab at the left side of the screen to login using your ID and password. Use your existing login or the "Register" button at the left to create a login, in order to gain access to many areas of the ITRC. Remember to save the User ID assigned to you, and your password.

In the left most frame select "Maintenance and Support".

Under the "Notifications" section (near the bottom of the page), select "Support Information Digests".

To –subscribe– to future HP Security Bulletins or other Technical Digests, click the check box (in the left column) for the appropriate digest and then click the "Update Subscriptions" button at the bottom of the page.

or

To –review– bulletins already released, select the link (in the middle column) for the appropriate digest.

NOTE: Using your itrc account security bulletins can be found here:

<http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin>

To –gain access– to the Security Patch Matrix, select the link for "The Security Bulletins Archive". (near the bottom of the page) Once in the archive the third link is to the current Security Patch Matrix. Updated daily, this matrix categorizes security patches by platform/OS release, and by bulletin topic. Security Patch Check completely automates the process of reviewing the patch matrix for 11.XX systems. Please note that installing the patches listed in the Security Patch Matrix will completely implement a security bulletin \_only\_ if the MANUAL ACTIONS field specifies "No."

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

The Security Patch Check tool can verify that a security bulletin has been implemented on HP-UX 11.XX systems providing that the fix is completely implemented in a patch with no manual actions required. The Security Patch Check tool cannot verify fixes implemented via a product upgrade.

For information on the Security Patch Check tool, see:  
[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)

The security patch matrix is also available via anonymous ftp:

[ftp://ftp.itrc.hp.com/export/patches/hp-ux\\_patch\\_matrix/](ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/)

On the "Support Information Digest Main" page:  
click on the "HP Security Bulletin Archive".

The PGP key used to sign this bulletin is available from several PGP Public Key servers. The key identification information is:

2D2A7D59

HP Security Response Team (Security Bulletin signing only)

<[security-alert@hp.com](mailto:security-alert@hp.com)>

Fingerprint =

6002 6019 BFC1 BC62 F079 862E E01F 3AFC 2D2A 7D59

If you have problems locating the key please write to [security-alert@hp.com](mailto:security-alert@hp.com). Please note that this key is for signing bulletins only and is not the key returned by sending 'get key' to [security-alert@hp.com](mailto:security-alert@hp.com).

D. To report new security vulnerabilities, send email to

[security-alert@hp.com](mailto:security-alert@hp.com)

Please encrypt any exploit information using the security-alert PGP key, available from your local key server, or by sending a message with a -subject- (not body) of 'get key' (no quotes) to [security-alert@hp.com](mailto:security-alert@hp.com).

---

(c)Copyright 2003 Hewlett-Packard Company  
Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.  
Hewlett-Packard Company and the names of HP products referenced herein are trademarks and/or service marks of Hewlett-Packard Company. Other product and company names mentioned herein may be

comp.security.misc: Potential Security Vulnerability in xdrmem\_getbytes() (rev.2)

trademarks and/or service marks of their respective owners.

---

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

Version: PGP Personal Security 7.0.3

iQA/AwUBPqWntOafOvwtKn1ZEQKyawCg1x3GrpW4rQHduI0o7a7BTpsG0dAAoJ7r  
o+oqBDrtsPYx642AzLoEIOMR  
=JLSN

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

--

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