CERT Advisory CA-2003-10 Integer overflow in Sun RPC XDR library routines

Original release date: March 19, 2003
Last revised: April 9, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Applications using vulnerable implementations of SunRPC-derived XDR libraries, which include

- Sun Microsystems network services library (libnsl)
- BSD-derived libraries with XDR/RPC routines (libc)
- GNU C library with sunrpc (glibc)

Overview

There is an integer overflow in the *xdrmem_getbytes()* function distributed as part of the Sun Microsystems XDR library. This overflow can cause remotely exploitable buffer overflows in multiple applications, leading to the execution of arbitrary code. Although the library was originally distributed by Sun Microsystems, multiple vendors have included the vulnerable code in their own implementations.

I. Description

XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. Such routines are commonly used in remote procedure call (RPC) implementations to provide transparency to application programmers who need to use common interfaces to interact with many different types of systems. The *xdrmem_getbytes()* function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation. Depending on how and where the vulnerable *xdrmem_getbytes()* function is used, subsequent problems like buffer overflows may result.

Researchers at eEye Digital Security discovered this vulnerability and have also published an advisory. This issue is currently being tracked as VU#516825 by the CERT/CC and as CAN-2003-0028 in the Common Vulnerabilities and Exposures (CVE) dictionary. Note that this vulnerability is similar to, but distinct from, VU#192995.

II. Impact

Because SunRPC-derived XDR libraries are used by a variety of vendors in a variety of applications, this defect may lead to a number of security problems. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information.

Specific impacts reported include the ability to crash the rpcbind service and possibly execute arbitrary code with root privileges. In addition, intruders may be able to crash the MIT KRB5 kadmind or cause it to leak sensitive information, such as secret keys.

III. Solution

Apply a patch from your vendor

Apply the appropriate patch or upgrade as specified by your vendor. See Appendix A below and the Systems Affected section of VU#516825 for further information.

Note that XDR libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are statically linked must be recompiled using patched libraries. Applications that are dynamically linked do not need to be recompiled; however, running services need to be restarted in order to use the patched libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated XDR/RPC libraries.
2. Restart any dynamically linked services that make use of the XDR/RPC libraries.
3. Recompile any statically linked applications using the patched or updated XDR/RPC libraries.

Disable access to vulnerable services or applications

Until patches are available and can be applied, you may wish to disable access to services or applications compiled with the vulnerable *xdrmem_getbytes()* function.

As a best practice, the CERT/CC recommends disabling all services that are not explicitly required.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain the vulnerabilities described in this report.

Cray, Inc.

Cray Inc. may be vulnerable and has opened spr's 724153 and 724154 to investigate.

Fujitsu

We are currently investigating how the vulnerability reported under VU#516825 affects the Fujitsu UXP/V O.S. We will update this statement as soon as new information becomes available.

GNU glibc

Version 2.3.1 of the GNU C Library is vulnerable. Earlier versions are also vulnerable. The following patches have been installed into the CVS sources, and should appear in the next version of the GNU C Library. These patches are also available from the following URLs:

> *http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/rpc/xdr.h.diff?r1=1.26&r2=1.27&cvsroot=glibc http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_mem.c.diff?r1=1.13&r2=1.15&cvsroot=glibc http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_rec.c.diff?r1=1.26&r2=1.27&cvsroot=glibc http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_sizeof.c.diff?r1=1.5&r2=1.6&cvsroot=glibc http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_stdio.c.diff?r1=1.15&r2=1.16&cvsroot=glibc*

```
2002-12-16  Roland McGrath

        * sunrpc/xdr_mem.c (xdrmem_inline): Fix argument type.
        * sunrpc/xdr_rec.c (xdrrec_inline): Likewise.
        * sunrpc/xdr_stdio.c (xdrstdio_inline): Likewise.

2002-12-13  Paul Eggert

        * sunrpc/rpc/xdr.h (struct XDR.xdr_ops.x_inline): 2nd arg
        is now u_int, not int.
        (struct XDR.x_handy): Now u_int, not int.
        * sunrpc/xdr_mem.c: Include .
        (xdrmem_getlong, xdrmem_putlong, xdrmem_getbytes, xdrmem_putbytes,
        xdrmem_inline, xdrmem_getint32, xdrmem_putint32):
        x_handy is now unsigned, not signed.
        Do not decrement x_handy if no change is made.
        (xdrmem_setpos): Check for int overflow.
        * sunrpc/xdr_sizeof.c (x_inline): 2nd arg is now unsigned.
        (xdr_sizeof): Remove cast that is now unnecessary, now that
        x_handy is unsigned.
```

[text of diffs available in the links included above --CERT/CC]

Hewlett-Packard Company

RE: HP Case ID SSRT2439

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

Hitachi

Hitachi's GR2000 gigabit router series - is NOT vulnerable.

Hitachi's HI-UX/WE2 - is NOT vulnerable, because it does not support RPC/XDR Library.

IBM Corporation

The AIX operating system is vulnerable to the issues discussed in CERT vulnerability note VU#516825 in releases 4.3.3, 5.1.0 and 5.2.0.

IBM provides the following official fixes:

> *APAR number for AIX 4.3.3: IY38524*
> *APAR number for AIX 5.1.0: IY38434*
> *APAR number for AIX 5.2.0: IY39231*

Please contact your local IBM AIX support center for any assistance.

Ingrian Networks

Ingrian Networks products are not succeptable to the vulnerabilities in VU#516825.

MIT Kerberos Development Team

It may be possible for a remote attacker to exploit an integer overflow in xdrmem_getbytes() to crash the kadmind server process by a read segmentation fault. For this to succeed, the kadmind process must be able to allocate more than MAX_INT bytes of memory. This is believed to be unlikely, as most installations are not likely to permit that the allocation of that much memory.

It may also be possible for a remote attacker to exploit this integer overflow to obtain sensitive information, such as secret keys, from the kadmind process. This is believed to be extremely unlikely, as there are unlikely to be ways for the information, once improperly copied, of being returned to the attacker. In addition, the above condition of the kadmind being able to allocate huge amounts of memory must be satisfied.

Please see http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-003-xdr.txt

This patch may also be found at:
http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt

The associated detached PGP signature is at:

http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt.asc

NEC Corporation

[Server Products] * EWS/UP 48 Series operating system - is NOT vulnerable.

NetBSD

The length types of the various xdr*_getbytes functions were made consistent somewhere back in 1997 (all u_int), so we're not vulnerable in that area.

[Note: the NetBSD project has released NetBSD Security Advisory 2003-008 in response to this issue --CERT/CC]

Network Appliance

NetApp products are not vulnerable to this issue.

Nokia

This issue has no relationship to the product we ship.

Nortel Networks

The following Nortel Networks Wireless products are potentially affected by the vulnerability identified in VU#516825:

CDMA SDMX
CS2000 SSPFS
GBMD (GSM Billing Mediation Device)
GSM CIPC
SS7IP Gateway
OAM&P Main & Performance Servers

Nortel Networks recommends applying the latest Sun Microsystems patches in accordance with that vendor's recommendations.

Other Nortel Networks products are being investigated to determine if they are potentially affected by the vulnerability identified in VU#516825 and this statement will be updated as more information becomes available.

Openwall GNU/*/Linux

The xdrmem_getbytes() integer overflow discovered by eEye Digital Security was present in the glibc package on Openwall GNU/*/Linux until 2003/03/23 when it was corrected for Owl-current (with a back-port from the glibc CVS) and documented as a security fix in the system-wide change log available at:

> *http://www.openwall.com/Owl/CHANGES-current.shtml*

Please note that Owl does not include any RPC services (but it does include a few RPC clients). It has not been fully researched whether an Owl install with no third-party software added is affected by this vulnerability at all.

SGI

SGI acknowledges receiving CERT VU#516825 and is currently investigating. This is being tracked as SGI Bug# 880925. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/

[Note: SGI has subsequently released SGI Security Advisory 20030402-01-P in response to this issue. Users are encouraged to review this advisory and apply the patches it refers to. --CERT/CC]

Sun Microsystems

Solaris 2.6, 7, 8 and 9 are vulnerable to VU#516825.

Sun will be publishing a Sun Alert for the issue at the following location shortly:
http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/51884

The Sun Alert will be updated with the patch information as soon as the patches are available.

At that time, the patches listed in the Sun Alert will be available from: http://sunsolve.sun.com/securitypatch

Top Layer Networks

Top Layer Networks products do not contain the vulnerabilities described in this CERT Advisory.

Appendix B. - References

1. AD20030318.html - http://www.eeye.com/html/Research/Advisories/AD20030318.html
2. VU#192995 - http://www.kb.cert.org/vuls/id/192995
3. VU#516825 - http://www.kb.cert.org/vuls/id/516825
4. RFC1831 - http://www.ietf.org/rfc/rfc1831.txt
5. RFC1832 - http://www.ietf.org/rfc/rfc1832.txt

Thanks to Riley Hassell of eEye Digital Security for discovering and reporting this vulnerability. Thanks also to Sun Microsystems for additional technical details.

Authors: Chad Dougherty and Jeffrey Havrilla

Revision History

```
Mar 19, 2003:  Initial release
Mar 20, 2003:  Updated vendor statement from Hitachi
Mar 24, 2003:  Added vendor statement for Openwall GNU/*/Linux
Apr 01, 2003:  Added vendor statement for Top Layer Networks, updated vendor statement for NetBSD
Apr 09, 2003:  Added vendor statement for Nortel Networks, updated vendor statement for SGI
```