

# [UNIX] QNX Neutrino RTOS libAp ABLPATH Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00033.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 9 Feb 2006 15:03:49 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

QNX Neutrino RTOS libAp ABLPATH Buffer Overflow Vulnerability

---

## SUMMARY

<A HREF="QNX Software Systems Ltd.'s Neutrino RTOS (QNX) is a real-time operating system designed for use in embedded systems. More information is available at:"> Software Systems Ltd.'s Neutrino RTOS (QNX) is a real-time operating system designed for use in embedded systems.

Local exploitation of a stack-based buffer overflow vulnerability in QNX Inc.'s Neutrino RTOS Operating System allows local attackers to gain root privileges.

## DETAILS

Vulnerable Systems:

- \* QNX Neutrino RTOS 6.3.0
- \* All versions are suspected vulnerable.

The vulnerability specifically exists due to improper handling of environment variables in the libAP system library. The libAP system library is utilized by various setuid applications, including all

## [UNIX] QNX Neutrino RTOS libAp ABLPATH Buffer Overflow Vulnerability

applications that are PhAB-generated. The `_ApFindTranslationFile()` function fails to check bounds on the ABLPATH environment variable prior to a `strcat` operation.

An attacker can supply an overly long value for ABLPATH to overflow the stack buffer and overwrite the return address as shown here:

Program received signal SIGSEGV, Segmentation fault.

0xb8242bf7 in ApMultiStrcat () from

/usr/qnx630/target/qnx6/x86/usr/lib/libAp.so.2

(gdb) x/i \$pc

0xb8242bf7 <ApMultiStrcat+15>: mov (%eax),%dl

(gdb) bt

#0 0xb8242bf7 in ApMultiStrcat () from

/usr/qnx630/target/qnx6/x86/usr/lib/libAp.so.2

#1 0xb823ce07 in \_ApFindTranslationFile () from

/usr/qnx630/target/qnx6/x86/usr/lib/libAp.so.2

#2 0x42424242 in ?? ()

Successful exploitation of the vulnerability allows local attackers to gain root privileges. The libAP library is a core system library on Neutrino RTOS, however it has had a number of trivial vulnerabilities similar to this one. A related vulnerability is the ABLANG environment variable overflow which results in a similarly exploitable scenario.

Workaround:

As a workaround solution, remove the setuid bit from any programs linked to libAP.so.2. An example is shown here:

```
# ls -l /usr/photon/bin/phlocale
-rwsrwxr-x 1 root root 54244 May 05 2004 /usr/photon/bin/phlocale
# ldd /usr/photon/bin/phlocale
/usr/photon/bin/phlocale:
libAp.so.3 => /usr/lib/libAp.so.3 (0xb8200000)
libph.so.3 => /usr/lib/libph.so.3 (0xb8210000)
libphrender.so.2 => /usr/lib/libphrender.so.2 (0xb8312000)
libm.so.2 => /lib/libm.so.2 (0xb8347000)
libfont.so.1 => /lib/libfont.so.1 (0xb8363000)
libc.so.2 => /usr/lib/ldqnx.so.2 (0xb0300000)
# chmod -s /usr/photon/bin/phlocale
```

Disclosure Timeline:

12/15/2005 – Initial vendor notification

02/07/2006 – Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=381>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=381>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.