

# [VulnWatch] iDefense Security Advisory 02.07.06: QNX Neutrino RTOS libAp ABLPATH Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00018.html>

---

- *From:* "labs-no-reply@xxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxx>
  - *Date:* Wed, 08 Feb 2006 10:46:52 -0500
- 

QNX Neutrino RTOS libAp ABLPATH Buffer Overflow Vulnerability

iDefense Security Advisory 02.07.06

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

February 7, 2006

## I. BACKGROUND

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:

<http://www.qnx.com/products/rtos/>

## II. DESCRIPTION

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

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 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 ?? ()
```

Attackers can supply a specially crafted value to overflow the buffer and execute arbitrary code.

### III. ANALYSIS

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.

### IV. DETECTION

iDefense has confirmed the existence of this vulnerability on QNX Neutrino RTOS 6.3.0. All versions are suspected vulnerable.

### V. 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
```

### VI. VENDOR RESPONSE

The vendor has not responded to communication regarding this issue.

### VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

### VIII. DISCLOSURE TIMELINE

12/15/2005 Initial vendor notification  
02/07/2006 Public disclosure

### IX. CREDIT

iDefense credits Filipe Balestra (filipe at balestra.com.br <<https://lists.grok.org.uk/mailman/listinfo/full-disclosure>>) with the discovery of this vulnerability.

Get paid for vulnerability research  
<http://www.idefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events  
<http://labs.idefense.com>

## X. LEGAL NOTICES

Copyright © 2006 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email customerservice at ideoense.com <<https://lists.grok.org.uk/mailman/listinfo/full-disclosure>> for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.