

[VulnWatch] iDefense Security Advisory 02.07.06: QNX Neutrino RTOS phgrafx Command Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00011.html>

- *From:* "labs-no-reply@xxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Tue, 07 Feb 2006 18:49:54 -0500
-

QNX Neutrino RTOS phgrafx Command Buffer Overflow

iDefense Security Advisory 02.07.06

<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=384>

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 buffer overflow in QNX Neutrino RTOS's (QNX) 'phgrafx' command allows attackers to gain root privileges.

The problem specifically exists in the parsing of a long string passed as the first argument to the set user id (setuid) binary 'phgrafx'. A string larger than approximately 1,000 bytes causes a stack overflow directly overwriting the stored return address and allowing an attacker to seize CPU control and eventually execute arbitrary code under root privileges.

III. ANALYSIS

Successful exploitation provides local attackers with super-user privileges on the affected system allowing for complete control.

IV. DETECTION

iDefense has confirmed the existence of these vulnerabilities in QNX Neutrino RTOS version 6.2.1. Earlier versions are suspected to be susceptible to exploitation as well.

V. WORKAROUND

Clear the set user id or execute bits from the affected binary or remove it entirely.

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

08/24/2004 Initial vendor notification

02/07/2006 Public disclosure

IX. CREDIT

Knud Hojgaard (<http://kohanin.dtors.net>) is credited with this discovery.

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@xxxxxxxxxxxxx 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.