

[VulnWatch] ptl-2004-03: WIDCOMM Bluetooth Connectivity Software Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/0462.html>

From: Pentest Security Advisories (*alerts_at_pentest.co.uk*)

Date: 08/11/04

Date: Wed, 11 Aug 2004 12:20:00 +0100

To: full-disclosure@lists.netsys.com, bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

Pentest Limited Security Advisory

WIDCOMM Bluetooth Connectivity Software Buffer Overflows

Advisory Details

Title: WIDCOMM Bluetooth Connectivity Software Buffer Overflows

Announcement date: 11 August 2004

Advisory Reference: ptl-2004-03

CVE Name: CAN-2004-0775

Products: WIDCOMM Bluetooth Connectivity Software

Vulnerability Type : Buffer Overflow

Vendor-URL: <http://www.widcomm.com>

Vendor-Status: Fixed in release 3.0

Remotely Exploitable: Yes

Locally Exploitable: N/A

Advisory URL: <http://www.pentest.co.uk/documents/ptl-2004-03.html>

Vulnerability Description

WIDCOMM's products provides a full range of Bluetooth connectivity solutions for PCs, PDAs, mobile phones, headsets, digital cameras, access points, and various output devices.

An unauthenticated remote attacker can submit various malformed service requests via Bluetooth, triggering a buffer overflow and executing arbitrary code on the vulnerable device.

On Windows platforms this allows arbitrary code execution under the context of the currently logged on user account.

Vulnerable Versions

WIDCOMM supply their Bluetooth Communications software to other

companies to allow them to integrate Bluetooth technology into their devices. They also supply Bluetooth SDK's to enable developers to create applications that use Bluetooth. Therefore it may not be immediately apparent that you are using the WIDCOMM Bluetooth software and version numbers may vary.

WIDCOMM's website (<http://www.widcomm.com/Partners/index.asp>) reports the following companies as customers or partners with WIDCOMM:

Logitech
Samsung Electro-Mechanics
Sony
Texas Instruments
Compaq Computer Corporation
Dell
National Semiconductor
Matsushita Electric Industrial Co., Ltd.
Wistron NeWeb Corporation
TDK Systems Europe
Zeevo
Cambridge Silicon Radio
Billionton
Broadcom Corporation
LG Innotek
MSI
Fujitsu Siemens Computers
Philips
Silicon Wave
Seiko Instruments Inc.
TECOM
Plantronics
Mobilian
Fujitsu Media Devices Limited
OKI Electric In