

# ptl-2004-03: WIDCOMM Bluetooth Connectivity Software Buffer Overflows

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-08/0155.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 Industry Co. Ltd.  
FIC  
Costar  
Brother  
Alcatel  
Atmel  
Conexant Systems, Inc.  
Microtune  
OSK

Pentest Limited have tested for the reported vulnerabilities against BTStackServer version 1.3.2.7 and 1.4.2.10 on both Windows XP and Windows 98 which ships with MSI Bluetooth Dongles. We have also tested this against an HP IPAQ 5450 running WinCE 3.0 with Bluetooth software version 1.4.1.03.

Pentest Limited have also written a proof of concept exploit for Windows XP.

## SecurityFocus Bugtraq: ptl-2004-03: WIDCOMM Bluetooth Connectivity Software Buffer Overflows

Whilst the above platforms are the only platforms tested and confirmed to be exploitable by Pentest Limited, discussions with the vendor lead us to believe that all versions prior to version BTW & BT-CE/PPC 3.0 are affected by this vulnerability.

WIDCOMM has not confirmed whether BT-PPC/Phone Edition, BT-Smartphone, BTE-Mobile or BTE are vulnerable.

### Vendor Status

#### WIDCOMM:

- 14-11-2003 – Initial Pentest Limited Notification
- 14-11-2003 – Notification acknowledged by WIDCOMM, request more detail
- 20-11-2003 – Pentest notify WIDCOMM of another vulnerability
- 06-01-2004 – Pentest send chase up Email without reply
- 13-01-2004 – Another email
- 13-01-2004 – WIDCOMM reply saying they are still working on it
- 21-01-2004 – Pentest email WIDCOMM that they have written a POC exploit
- 23-01-2004 – WIDCOMM reply saying they have resolved issue and fix will be available in next release.
- 10-02-2004 – Pentest ask for an update on expected release date
- 11-02-2004 – WIDCOMM plan February/early March release date
- 29-03-2004 – Pentest ask for update
- 12-05-2004 – Pentest ask for update
- 12-07-2004 – Pentest send chase up Email without reply
- 26-07-2004 – Pentest ask whether a patches will be released for older versions
- 03-08-2004 – WIDCOMM respond. No date set for new release and no patch will be made available for older versions.

### Fix

---  
Until version 3 of the WIDCOMM software becomes available from WIDCOMM or their customers/partners Pentest Limited recommend that end users stop using the vulnerable WIDCOMM Bluetooth software or set their Bluetooth device configuration to be non-discoverable or hidden. This will not stop the device from being vulnerable but it may limit the exposure.

Credit

-----  
These vulnerabilities were discovered by Mark Rowe and Matt Moore from Pentest Limited.