Security Advisory	mobilesecuritylab
MSL-2008-002 HTC Touch vCard over IP Denial of Service	

Advisory Information

Title	HTC Touch vCard over IP Denial of Service
Advisory ID	MSL-2008-002
Advisory URL	http://www.mseclab.com/index.php?page_id=110
Published	2008-12-19
Updated	2008-12-19
Vendor	HTC
Platforms	Touch Pro, Touch Cruise

Vulnerability Details

Class	Denial of Service
Remote	Yes
Local	No
Public References	Not Assigned
Affected	HTC Touch Pro HTC Touch Cruise
Not Affected	Currently Unknown
Description	UDP/9204 port is open and reachable both via WiFi and GPRS/UMTS connection when the device is capable of sending and receiving SMS. Port is always open on the Touch Pro, while on Touch Cruise the port is open when the SMS application is running. UDP/9204 is associated with the service WAP-vCard and is used for sending vCard files to the device, that are displayed as normal SMS to users. By flooding the device with multiple vCards it is possible to perform a Denial of Service attack that affects usability, SMS handling and connectivity. By sending large number of vCards an attacker can achieve significant device slowdown, making the UI sluggish and hard to use. In some cases WiFi connections may be dropped (when vCards are sent via WiFi), effectively disconnecting the device from the network.

	On Touch Cruise devices, SMS inbox can be completely filled by sending more then 450 large vCards (size 32K). The device will not be able to receive SMS anymore or to access the message stored inside the device until SMS deletion occurs. Additionally, when large vCards are sent, no acoustic notification (ring tones) will be played upon incoming messages, making the attack more silent and less noticeable by an user. Battery removal may be needed, in some cases, for restoring normal functionalities. Manual deletion of all received SMS requires a very long time, making the deletion of all the SMS the most viable option, but leading to loss of all received SMS and requiring in any case a large amount of time (even hours). The faster option for restoring the device is performing a hard reset of the device, leading to the loss of all the content saved on the handset. The attack can be easily carried in all the scenarios where the device IP stack is accessible to an attacker, such as Wireless LANs and Mobile Networks assigning public IP addresses without any firewall protection.
Solutions & Workaround	A personal firewall solution can be used for denying unwanted access to the port, effectively avoiding possible attacks.

Additional Information

Timeline	*2008-12-03:* Issue discovery *2008-12-05:* Initial Vendor Notification: Point of Contact requested via contact form on website (No suitable e-mail available) *2008-12-14:* Vendor Response: Customer support answered without providing any suitable contact for vulnerability communication *2008-12-19:* Public Disclosure
Vendor Statement	None