

4 January 2007

By: Sergiu Gatlan, Communications News Editor

[How to Exploit A Windows Mobile Handset](#)

By sending an MMS.

Yes, we all thought we were safe while browsing around the web on our [Windows Mobile](#) powered handsets. I am also one of the guys that had the false impression the world was safe for the WM owners but, today, I found out this certainty of mine was totally wrong. As I discovered, way back in August 2006, one of the team members from Trifinite Group named Collin Mulliner discovered a MMS exploit for the Windows Mobile operating systems and immediately after, he informed Microsoft about the vulnerabilities. Even if he did the right thing and didn't keep it a secret, Microsoft didn't send him any type of feed-back for the next six months so Collin went public with the exploit at the 23rd Chaos Communication Congress in Berlin. The proof-of-concept exploit presented at the Congress targets vulnerabilities in the way the Windows Mobile 2003 OS deals with the Synchronized Multimedia Integration Language (SMIL) protocol and creates a buffer overflow that will eventually lead to some type of arbitrary code execution that will give the exploiter the opportunity to run commands on the affected [device](#). The research led until now by Collin Mulliner has revealed that the only devices that seem to be affected by the proof-of-concept exploit he has presented in Berlin are our old acquaintances-the [i-mate](#) PDA2K and the HP iPaq h6315. Fortunately, the exploit will not enable the eventual attackers to run any type of code on the above mentioned devices because even in these cases, the one using the exploit will have to know the correct memory slot where the MMS processing code is executed and how to send the correct exploit code. What do all these mean? They mean the MMS message containing the malicious code arriving on your device will, at best, be able only to crash it and in no way will it leave a door open on to your handheld to an eventual attacker. As Jarno Niemela, a researcher at the F-Secure's Labs, has said, "while Collin's discovery is very significant, it does not pose immediate danger to any large group of users. And although it is possible to create an MMS worm or other malware that uses the vulnerability, this particular exploit cannot be directly used in creating malware". So, beware and keep your Windows Mobile devices updated because you never now from where a MMS will come and crash your OS to the ground. Just kidding for now but we will have to wait and see what the future will prepare for us. I have a very bad feeling about it!