

[NT] Pocket Controller Professional Unauthorized Access Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00039.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2005 17:14:10 +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>

Pocket Controller Professional Unauthorized Access Vulnerability

SUMMARY

<<http://www.soti.net/>> Pocket Controller – "provides mobile device users with the tools they need to remotely control and manage their device(s) from a desktop/notebook computer over wireless or wired connections."

A vulnerability discovered in Pocket Controller professional allows remote attackers to turn off, reboot or "hard reset" a PDA running the vulnerable software.

DETAILS

Vulnerable Systems:

- * Pocket Controller Professional version 5.0 and prior

Lack of authentication in the control management allows malicious remote attacker to turn off, reboot, or hard reset a vulnerable PDA by sending certain packets via a wireless connection to the PDA on port 5492.

Proof of concept:

1. Connect to port 5492 on PDA that is running the target client program.

[NT] Pocket Controller Professional Unauthorized Access Vulnerability

2. Send an initialization packet to the PDA.
3. Send a packet containing the desired command (turn off, reboot, hard reset) to the PDA.
4. Create a new socket and reset the initialization packet.
5. Upon receipt, the PDA will perform the selected function.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.airscanner.com/security/pocketcontroller.htm>>

<http://www.airscanner.com/security/pocketcontroller.htm>

=====

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@xxxxxxxxxxxxxxx

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

=====
=====

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.

-
- Prev by Date: [*\[NEWS\] Gecko InstallVersion.compareTo Code Execution \(Exploit\)*](#)
 - Next by Date: [*\[EXPL\] SimpleBBS Command Execution \(Exploit\)*](#)
 - Previous by thread: [*\[NEWS\] Gecko InstallVersion.compareTo Code Execution \(Exploit\)*](#)
 - Next by thread: [*\[EXPL\] SimpleBBS Command Execution \(Exploit\)*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)