

# [NEWS] ACT P202S VoIP Wireless Phone Multiple Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00060.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 19 Jan 2006 17:17:48 +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>

-----

ACT P202S VoIP Wireless Phone Multiple Vulnerabilities

---

## SUMMARY

Multiple undocumented open ports in ACT P202S wireless VoIP phone allow attackers to remotely login to the phone, retrieve phone information and DoS it.

## DETAILS

Vulnerable Systems:

- \* ACT P202S Firmware version 1.1.21 on VxWorks

The ACT P202S VoIP 802.11b wireless phone, version 1.01.21 on VxWorks has three undocumented ports and extraneous services that can be exploited by attackers.

1. Undocumented port, UDP/17185 VxWorks WDB remote debugging (wdbrpc) allow attackers direct access to the phone memory and OS internals.
2. Undocumented port, TCP/7 echo allow attackers to reflect sent network data using the echo service, causing a DoS.
3. Undocumented port, TCP/513 rlogin allow attackers to rlogin access with no need for credentials.

[NEWS] ACT P202S VoIP Wireless Phone Multiple Vulnerabilities

4. Hardcoded NTP server in the phone configuration for Taiwan NTP server.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:shawnmer@xxxxxxxxxx>> Shawn Merdinger.

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

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: [\*\[EXPL\] Veritas NetBackup Module Stack Overflow \(vmd, Exploit\)\*](#)
  - Next by Date: [\*\[TOOL\] iWar PSTN Auditing Tool\*](#)
  - Previous by thread: [\*\[EXPL\] Veritas NetBackup Module Stack Overflow \(vmd, Exploit\)\*](#)
  - Next by thread: [\*\[TOOL\] iWar PSTN Auditing Tool\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)