

# [NT] Trend Micro PC-Cillin Internet Security Insecure File Permission

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00045.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 15 Dec 2005 14:06:16 +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>

-----

Trend Micro PC-Cillin Internet Security Insecure File Permission

---

## SUMMARY

"

<<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>> Trend Micro PC-cillin Internet Security combines award-winning Antivirus security and a personal firewall for comprehensive protection against viruses, worms, Trojans, and hackers."

Local exploitation of an insecure permission vulnerability in multiple Trend Micro PC-cillin Internet Security allows attackers to escalate privileges or disable protection.

## DETAILS

### Vulnerable Systems:

- \* Trend Micro PC-Cillin Internet Security 2005 version 12.00 build 1244.

### Immune Systems:

- \* Trend Micro PC-Cillin Internet Security 2005 version 12.4

The vulnerabilities specifically exist in the default Access Control List (ACL) settings that are applied during installation. When an administrator

[NT] Trend Micro PC-Cillin Internet Security Insecure File Permission

installs an affected Trend Micro product, the default ACL allows any user to modify the installed files. Due to the fact that some of the programs run as system services, a user could replace an installed Trend Micro product file with their own malicious code, and the code would be executed with system privileges.

Successful exploitation allows local attackers to escalate privileges to the system level. It is also possible to use this vulnerability to simply disable protection by moving all of the executable files so that they cannot start upon a reboot. Once disabled, the products are no longer able to provide threat mitigation, thus opening the machine up to attack.

Workaround:

Apply proper Access Control List settings to the directory that the affected Trend Micro product is installed in. The ACL rules be set so that no regular users can modify files in the directory.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3360>>  
CVE-2005-3360

Disclosure Timeline:

- 10/27/2005 – Initial vendor notification
- 10/27/2005 – Initial vendor response
- 12/14/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://www.iddefense.com/application/poi/display?id=351&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=351&type=vulnerabilities>

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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: [\*\[NEWS\] Land Attacks Still Going Strong\*](#)
- Next by Date: [\*\[NT\] Microsoft Office InfoPath 2003 Form Handling DoS\*](#)
- Previous by thread: [\*\[NEWS\] Land Attacks Still Going Strong\*](#)
- Next by thread: [\*\[NT\] Microsoft Office InfoPath 2003 Form Handling DoS\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)