

[NEWS] Yahoo! Webcam ActiveX Control Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0067.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/21/03

To: list@securiteam.com

Date: 21 Sep 2003 13:01:02 +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>

Yahoo! Webcam ActiveX Control Buffer Overflow

SUMMARY

Yahoo! Webcam Viewer Wrapper is an ActiveX control used by Webcam feature of Yahoo! Messenger and Yahoo! Chat also it can be installed from Internet as a stand-alone ActiveX control. This ActiveX control has a heap based overflow vulnerability.

DETAILS

When a long value is set in Yahoo! Webcam Viewer Wrapper ActiveX control's "TargetName" property a stack and heap based buffer overflow occurs depending on the length of the string.

To reproduce the overflow just cut-and-paste the following:

-----sample.htm-----

```
< object id="yahoowebcam"
classid="CLSID:E504EE6E-47C6-11D5-B8AB-00D0B78F3D48" >
</object>
< script>
yahoowebcam.TargetName="longstringhere";
```

Securiteam: [NEWS] Yahoo! Webcam ActiveX Control Buffer Overflow

</script>

As this ActiveX control is marked as safe, the above sample will run without being blocked in default Internet Explorer security configuration. This vulnerability can be exploited to run arbitrary code.

Workaround:

If you have installed the ActiveX from Internet as a stand-alone ActiveX control or you have used Yahoo! Chat then:

- * Go to: %SystemRoot%\Downloaded Program Files\
- * Right Click on: Yahoo! Webcam Viewer Wrapper
- * Left Click: Remove

Patch:

By going to: <<http://messenger.yahoo.com/messenger/security/>>
<http://messenger.yahoo.com/messenger/security/> Yahoo! Messenger will prompt to update upon sign-in.

ADDITIONAL INFORMATION

The information has been provided by Cesar Cerrudo.

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

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.