

[NT] ICQ 6 Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-04/msg00044.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 16 Apr 2008 21:53:40 +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 6 Buffer Overflow Vulnerability

SUMMARY

ICQ (I Seek You) Instant Messenger is "one of the most popular internet chat software. Since 1996, it has grown to a community of over 180 million users. It has features for instant messaging, chat, sending e-mail, SMS, file transfer, wireless-pager messages, etc".

INFIGO IS's security team identified a critical remote buffer overflow vulnerability in the latest ICQ version (ICQ 6.0). In newer versions, ICQ has a 'Personal Status Manager' feature, where a user can specify text messages for his status/mood (online/offline/etc.). The specified message will be visible in the title part of a remote user's ICQ chat window, when a chat session is initiated.

DETAILS

Vulnerable Systems:

* ICQ version 6 (build 6043)

When a user writes a message in the status manager, the text string is processed with the boxelyRenderer module. The boxelyRenderer module has a vulnerability in the HTML tags processing code. If malformed HTML tags are

[NT] ICQ 6 Buffer Overflow Vulnerability

set for the 'status message', boxelyRenderer will try to process the HTML tags, and a UNICODE heap overflow will occur.

The 'status' string from a remote user is processed by boxelyRenderer for each new chat session. If the remote user has a malicious 'status message', ICQ's heap memory will be overflowed.

Upon setting, the status message is sent to ICQ's servers, and will be stored on them. When another user looks up the malicious user's profile, or tries to send him a message, even if the malicious user is offline, the ICQ client will receive the malicious status message from ICQ's server. In other words, once the malicious user sets his status message, he doesn't have to be online in order to exploit other vulnerable ICQ clients.

There are few different exploitation paths for this vulnerability, and they depend on user actions in ICQ and the current heap state.

Below is an example of malicious HTML code that will crash ICQ:

```
<a href="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" ></a>
```

When a user sets this HTML code as his 'status message', ICQ/boxelyRenderer will process it and ICQ will crash. To prevent this, open ICQ in debugger and set it to ignore INT3 and memory violation exceptions.

We identified two exploitable scenarios:

Scenario 1:

In this scenario, the ESI register has our input, so we control the EIP register at the 'CALL' instruction.

boxelyRE:

```
-----  
MOV EDX, DWORD PTR DS:[ESI]  
PUSH 5A  
LEA EAX, DWORD PTR SS:[EBP-2A0]  
PUSH EAX  
MOV ECX, ESI  
CALL DWORD PTR DS:[EDX+8] <- HERE  
-----
```

Scenario 2:

In this scenario, which is harder to exploit, we can write one byte to a memory location.

ntdll:

```
MOV BYTE PTR DS:[EDI+6], AL
```

Fix:

The vendor has addressed this vulnerability on 1st of March 2008 with an

[NT] ICQ 6 Buffer Overflow Vulnerability

automatic update.

Vendor status:

- 26.02.2008 – Initial contact
- 26.02.2008 – Initial vendor response
- 28.02.2008 – Further clarification about the vulnerability
- 28.02.2008 – Vendor status update
- 01.03.2008 – Vendor released an automatic update.
- 14.03.2008 – Vendor status update
- 14.04.2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:infocus@xxxxxxxxxx>> infocus.
The original article can be found at:
<http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-04-08>
http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-04-08

=====

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

=====
=====

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.