

[Full-disclosure] EYE: Yahoo Webcam ActiveX Controls Multiple Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-06/msg00189.html>

- *From:* "eEye Advisories" <Advisories@xxxxxxxx>
 - *Date:* Fri, 8 Jun 2007 10:58:08 -0700
-

Yahoo Webcam ActiveX Controls Multiple Buffer Overflows

Release Date:
June 8, 2007

Date Reported:
June 5, 2007

Severity:
High (Remote Code Execution)

Vendor:
Yahoo!, Inc.

Systems Affected:
Yahoo Messenger 8 for Windows

Overview:
eEye Digital Security has discovered two critical vulnerabilities in ywcupl.dll (version 2.0.1.4) and ywcvwr.dll (version 2.0.1.4) included by default in all releases of Yahoo! Messenger 8.x. Ywcupl.dll is Yahoo's Webcam Upload ActiveX Control used by Yahoo! Messenger to stream content from a user's webcam to other users. Ywcvwr.dll is Yahoo! Messenger's Webcam Viewer ActiveX Control used to view any streamed content. These files are normally used only when viewing or streaming webcam content to and from Yahoo Messenger, but they are incorrectly marked safe for scripting and can be instantiated by any website. Furthermore they both fail to perform bounds checking on variables resulting in 2 stack-based buffer overflow conditions that could allow arbitrary code to execute in the context of the logged-in user.

The vulnerability is a simple strcpy-based stack buffer overflow within the ActiveX controls, and can be reliably exploited on all versions of Windows in order to execute arbitrary code.

Technical Details:
The code for both vulnerabilities is similar, in which they both call mbscpy on the vulnerable string after allocating only 1023 bytes of

[Full-disclosure] EEEY: Yahoo Webcam ActiveX Controls Multiple Buffer Overflows

space.

```
03ada506 or dword ptr [ebp-4],0FFFFFFFFh
03ada50a cmp eax,ebx
03ada50c mov dword ptr [esi+210h],eax
03ada512 je ywcupl+0xa5f4
03ada518 lea ecx,[esi+174h]
; Loads the payload into ECX
03ada51e call dword ptr
[ywcupl!DllUnregisterServer+0x4b44
7c3a44b3 cmp dword ptr [ecx+18h],10h
7c3a44b7 jb MSVCP71!std::basic_string
<char,std::char_traits<char>,std::allocator<char>>::_Myptr+0xa
(7c3a44bd)
7c3a44b9 mov eax,dword ptr [ecx+4]
; Payload is in EAX
7c3a44bc ret
03ada524 push eax
; push payload to the stack
03ada525 push 3FFh
; Max size of 1023
03ada52a lea eax,[ebp-414h]
; EAX = 159dfb98

; (Destination buffer Location)
03ada530 push eax

03ada531 push offset ywcupl!DllUnregisterServer+0x6498;
"WebcamServer" gets

; pushed on the stack
03ada536 lea ecx,[esi+0F8h]
; ECX loads payload
03ada53c call ywcupl+0x4a72
....
03ad4ac1 push dword ptr [ebp+14h]
; pushes our payload to the stack
03ad4ac4 push dword ptr [ebp+0Ch]
; pushes 0x159dfb98

; (Destination Buffer to copy payload)
03ad4ac7 call ywcupl!DllUnregisterServer+0x28f2
(03aebfa6)
03aebfa6 jmp dword ptr
[ywcupl!DllUnregisterServer+0x4b9c] ; Call MSVCR71!mbscopy
```

At this point either of the vulnerable ActiveX controls call mbscopy without bounds checking the 'server' string variable. If this variable

[Full-disclosure] EEYE: Yahoo Webcam ActiveX Controls Multiple Buffer Overflows

is excessively large it causes a page boundary access violation upon reaching the bottom of the stack.

After hitting a page boundary the exception handler gets called and attempts to clean up the access violation. Since the stack has been overflowed with a payload, the exception handler loads the payload and calls it in the following code:

```
7c9037ae push dword ptr [ebp+14h]
7c9037b1 push dword ptr [ebp+10h]
7c9037b4 push dword ptr [ebp+0Ch]
7c9037b7 push dword ptr [ebp+8]
7c9037ba mov ecx,dword ptr [ebp+18h]
; ECX loads payload
7c9037bd call ecx
; Calls payload
```

Protection:

Retina – Network Security Scanner has been updated to identify this vulnerability.

Blink – Unified Client Security has proactively protected from this vulnerability since its discovery.

Vendor Status:

Yahoo! has released a patch for this vulnerability which is available at:

http://messenger.yahoo.com/security_update.php?id=060707

Credit:

Greg Linares

Related Links:

Retina – Network Security Scanner – Free Trial:

<http://www.eeye.com/html/products/retina/download/index.html>

Blink – Unified Client Security Personal – Free For Home Use:

<http://www.eeye.com/html/products/blink/personal/download/index.html>

Blink – Unified Client Security Professional – Free Trial:

<http://www.eeye.com/html/products/blink/download/index.html>

Greetings:

Terrell Karlsten, Dre, the Super Soeder Bros, Matt, Laurentiu, Richard D. James, Pikey, Cash, Expanders, Str0ke, William Kurnik, Big Perm, Dooritto, CSam, Shadow Penguin, and Reverse. Best of luck to where ever the winds may take you.

Copyright (c) 1998–2007 eEye Digital Security

Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express

[Full-disclosure] EEYE: Yahoo Webcam ActiveX Controls Multiple Buffer Overflows

consent of eEye. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please email alert@xxxxxxx for permission.

Disclaimer

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties, implied or express, with regard to this information. In no event shall the author be liable for any direct or indirect damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>