

# [NT] Apple QuickTime H.264 Integer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00015.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 13 Sep 2006 10:33:14 +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>

-----

Apple QuickTime H.264 Integer Overflow

---

## SUMMARY

By carefully crafting a corrupt H.264 movie, an attacker can trigger an integer overflow which may lead to an application crash or arbitrary code execution with the privileges of the user. The vulnerability allows an attacker to execute arbitrary code in the context of the user who executes QuickTime.

## DETAILS

Vulnerable Systems:

- \* Apple QuickTime version 7.1.2 and prior

Immune Systems:

- \* Apple QuickTime version 7.1.3

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4381>>  
CVE-2006-4381

This vulnerability exists in the way QuickTime process the H.264 content.

## [NT] Apple QuickTime H.264 Integer Overflow

Vulnerable code:

QuickTimeH264.qtx.68169AC3

```
text:68169A63 and esp, 0FFFFFFF8h
text:68169A66 sub esp, 214h
text:68169A6C mov eax, dword_68323140
text:68169A71 mov edx, [ebp+arg_8]
text:68169A74 xor ecx, ecx
text:68169A76 mov [esp+214h+var_4], eax
text:68169A7D mov eax, [ebp+arg_0]
text:68169A80 mov cl, [eax+4]
text:68169A83 push ebx
text:68169A84 push esi
text:68169A85 push edi
text:68169A86 mov [esp+220h+var_20C], 0
text:68169A8E and ecx, 3
text:68169A91 inc ecx
text:68169A92 mov [edx], ecx
text:68169A94 mov cl, [eax+5]
text:68169A97 and cl, 1Fh
text:68169A9A cmp cl, 1
text:68169A9D jnz short loc_68169AEF
text:68169A9F mov cx, [eax+6]
text:68169AA3 movzx dx, ch
text:68169AA7 mov dh, cl
text:68169AA9 mov ecx, edx
text:68169AAB cmp cx, 100h <-- cx = FFFF which is user controllable
text:68169AB0 jg short loc_68169AEF <-- should be "ja"
text:68169AB2 movsx edx, cx
text:68169AB5 mov ecx, edx
text:68169AB7 mov ebx, ecx <-- ecx = 0xFFFFFFFF
text:68169AB9 shr ecx, 2
text:68169ABC lea esi, [eax+8]
text:68169ABF lea edi, [esp+220h+var_208]
text:68169AC3 rep movsd <-- do memory copy
text:68169AC5 mov ecx, ebx
text:68169AC7 and ecx, 3
text:68169ACA rep movsb
text:68169ACC mov cl, [edx+eax+8]
text:68169AD0 lea esi, [edx+8]
text:68169AD3 inc esi
text:68169AD4 cmp cl, 1
text:68169AD7 jnz short loc_68169AEF
text:68169AD9 mov cx, [esi+eax]
text:68169ADD movzx bx, ch
text:68169AE1 mov bh, cl
text:68169AE3 add esi, 2
text:68169AE6 mov ecx, ebx
text:68169AE8 cmp cx, 100h
text:68169AED jle short loc_68169B07
```

## [NT] Apple QuickTime H.264 Integer Overflow

This vulnerability can be exploited By persuading a user to open a carefully crafted .mov files or visit a website embedding the malicious mov file.

### Vendor Response:

2006.05.06 – Vendor notified via product–security@xxxxxxxxxx  
2006.05.07 – Vendor responded  
2006.09.07 – Vendor notified me the patch is available.  
2006.09.12 – Vendor released QuickTime 7.1.3  
2006.09.12 – Advisory released

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:smailist@xxxxxxxxxx>> Sowhat.  
The original article can be found at:  
<<http://secway.org/advisory/AD20060912.txt>>  
<http://secway.org/advisory/AD20060912.txt>

=====

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.