threatpost
The Kaspersky Lab Security News Service

August 30, 2010, 1:37PM

New Remote Flaw in Apple QuickTime Bypasses ASLR and DEP (/en_us/blogs/new-remote-flaw-apple-quicktime-bypasses-aslr-and-dep-083010)

by Dennis Fisher (/author/Dennis Fisher)
Follow @DennisF

0

(http://threatpost.com/en_us/blogs/new-remote-flaw-apple-quicktime-bypasses-aslr-and-dep-083010) A Spanish security researcher has discovered a new vulnerability in Apple's QuickTime software that can be used to bypass both ASLR and DEP on current versions of Windows and give an attacker control of a remote PC. The flaw apparently results from a parameter from an older version of QuickTime that was left in the code by mistake.

The flaw was discovered by Ruben Santamarta (http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1) of Wintercore, who said that the vulnerability can be exploited remotely via a malicious Web site. On a machine running Internet Explorer on Windows 7, Vista or XP with QuickTime 7.x or 6.x installed, the problem can be exploited by using a heap-spraying technique. In his explanation of the details of the vulnerability and the exploit for it, Santamarta said that he believes the parameter that is at the heart of the problem simply was not cleared out of older versions of the QuickTime code.

The result of the problem is the creation of what amounts to a backdoor in the QuickTime code, Santamarta said. "WATCH OUT! Do not hype this issue beyond it deserves. This time Backdoor != malicious code but a horrible trick a developer implemented during the development cycle.These hacks could end up having a harmful impact," he wrote in his blog post explaining the vulnerability.

Santamarta has sent the exploit code to the folks at the Metsploit Project and there will be a Metasploit module available for this attack soon.

"The Quicktime plugin is widely installed and exploitable through IE; ASLR and DEP are not effective in this case and we will likely see this in the wild," said HD Moore, founder of the Metasploit Project.

Moore added that it looks right now as though the bug is exploitable only through Internet Explorer, and is likely to be exploited through drive-by download attacks.

Editor's Pick

Attorney General: Massachusetts Won't Investigate iTunes Fraud (/en_us/blogs/attorney-general-massachusetts-wont-investigate-itunes-fraud-101711)

Apple Ships Mammoth Security

Update for OS X (/en_us/blogs/apple-ships-mammoth-security-update-101311)

Massachusetts Attorney General, Victim of an iTunes Scam, Says She'll Demand Answers (/en_us/blogs/massachusetts-attorney-general-victim-itunes-scam-says-shell-demand-answers-092111)

Threatpost Newsletter Sign-up *(/en_us/node/1690)*

From Santamarta's advisory:

> Reversing this function we can see that, in certain cases, QTPlugin.ocx could be instructed to draw contents onto an existing window instead of creating a new one. Mistery [sic] solved. However, although this functionality was removed in newer versions, the param is still present. Why? I guess someone forgot to clean up the code .
>
> We are controlling the IStream Pointer passed to CoGetInterfaceAndReleaseStream, at a certain point during the execution flow of this function, an IStream method is going to be referenced.
>
> ole32!wCoGetInterfaceAndReleaseStream -> ole32!CoUnmarshalInterface -> ole32!ReadObjRef -> **ole32!StRead** < = p0wn!!
>
> So all we need to do is emulate a fake IStream interface in memory. How? aligned heap spray FTW!

Santamarta's exploit involves creating a fake pointer in memory aas part of the heap-spraying technique.

"As you can see a couple of gadgets are used, since this is a ROP exploit, however esp is not controlled at all. I'm taking advantage of common code generated by c++ compilers to control parameters and execution. The gadgets come from Windows Live messenger dlls that are loaded by default on IE and have no ASLR flag," Santamarta said in his advisory.

Santamarta was one of the researchers who, in parallel with Tavis Ormandy, discovered a serious bug in Java (http://threatpost.com/en_us/blogs/serious-new-java-flaw-affects-all-browsers-040910) in April.

Commenting on this Article is closed.

Comments

Submitted by Anonymous (not verified) on Mon, 08/30/2010 - 7:15pm.

Until then, I guess the only mitigation is to block *.mov from working in our browsers with a reg exp.

Submitted by Anonymous (not verified) on Mon, 08/30/2010 - 7:12pm.

I sure hope Apple can restore the broken .mov file support in Sony Vegas 8 pretty soon, from their last two quicktime updates.

Some of us Vegas 8 users out here had to skip the last two updates, and risk getting exploited, all so we might still be productive.

Submitted by Anonymous (not verified) on Tue, 08/31/2010 - 12:49am.

Cool--maybe this will finally be the big downfall of IE...after all, if I had to chose between QT support and IE, I'm out the door for Firefox...

Submitted by Senki Alfonz (not verified) on Tue, 08/31/2010 - 4:19am.
It appears this flaw was irresponsibly disclosed, that is, the vendor was not consulted for producing a hotfix before dumping the details on the web. I think sw vendors should refuse to fix irresponsibly disclosed bugs or exploits and direct users to do whatever they want to the hackers in retaliation. Maybe corporates should even have a policy of hunting down vxers and hackers, who publish zero days. I can't see why a big company, richer than many small countries, shouldn't have the authority to dispose of their enemies with impunity, in the same way any small country can, if they have a secret service.

Submitted by Anonymous (not verified) on Sun, 01/16/2011 - 10:16pm.

freedom of speech. releasing vuln and exploit only improves security awareness. go to the corporate world

> where people stick their in the ground like some birds when they see trouble... who cares about responsible disclosure? last I checked, these security researchers do not get paid to be responsible with disclosures, they would be wasting their time. would you code a module to improve performance on quicktime and then give it to them for free? its the responsible thing to do, doesnt it improve the program for everyone? of course you would not -- show me the money. responsible disclosure is something that security white hats have come up with to give themselves jobs and credits. without responsible disclosure, programs for policy based compliance will not exist. e.g. vulnerability management scanners etc. but put cves and advisory ID's and now you have a new economy for indepedent researchers and companies.

Submitted by Anonymous (not verified) on Tue, 08/31/2010 - 12:21pm.

boy is Senki every a mac fan...

Submitted by Johannes Rexx (not verified) on Wed, 09/01/2010 - 12:42am.

So we are currently at QuickTime X and not the ages-old versions 6 or 7, so it's not clear to me exactly why this is newsworthy. I heard that a long time ago some vendor's early IP stack was susceptible to the "ping of death" so now everybody blocks ICMP. Why are we *still* closing the barn door long after the horse has escaped?

Submitted by Anonymous (not verified) on Wed, 09/01/2010 - 10:12am.

people dont block icmp just because of the ping of death

Submitted by Anonymous (not verified) on Thu, 09/02/2010 - 7:33am.

Senki Alfonz says, "It appears this flaw was irresponsibly disclosed, that is, the vendor was not consulted for producing a hotfix before dumping the details on the web."

I don't care too much about that. Ultimately not even a GOD (of your choice) can stop people from disclosing things.

What bothers me is Apple Quicktime security updates (The last TWO) broke .mov file support in Sony Vegas 8 Pro . If your low budget, and trying to keep secure, producing work this is a real no starter. I hope everyone starts trying to keep the economy going not sabotage it.

I have cloned the OS, so I was able to roll back. Other's maybe not so lucky?

Come on Apple fix this thing if your reading. please.

Ultimately, this dll thing is because of a port being open (if I am not mistaken) so theoretically by blocking this webdav ports say 130 - 7000 no more webdav, no more BS right? Understand too, some people can only afford to spend so much money and time on security, until the security becomes more of a job than actually getting work done. In some cases a video editing workstation must have access to the web for information flowing in and out. And considering Murphy's law, the thing we want to block "quicktime .mov. .mpg" just happens to be the same thing we are now crippling at the production level.

Making apple worse than the initial threat by leaving the system "back to the stone age" after update.

It's frankly a pain in the ass for artists to keep up with all this cruft.