

Forum:[Hack Forums](#)

Thread: [Full info on Latest Java 0day Exploit](#)

Antigen - August 29, 2012, 11:06 am

I hope you all heard of Latest Java 0day Exploit, Got info on it.

Here is some news reports(Exploit hits the Web internationally, All versions of 7.xxx java is affected)

http://www.theregister.co.uk/2012/08/27/disable_java_to_block_exploit/

<http://www.h-online.com/open/news/item/Java-0Day-Turn-off-Java-applets-now-1678618.html>

Currently there is only one way to prevent infection by DISABLE JAVA right now, (Wait for Oracle releases a patch or update)

Update: Some AVs (Kaspersky, Sophos) is now prevent loading infected websites.

To Turn off Java in Mozilla

At the top of the Firefox window, click on the Firefox button (Tools menu in Windows XP), and then click Add-ons. The Add-ons Manager tab will open

In the Add-ons Manager tab, select the Plugins panel.

Click on the Java ™ Platform plugin to select it.

Click on the Disable button (if the button says Enable, Java is already disabled).

Java applets will no longer be permitted to launch in Firefox.

To Turn off Java in Chrome

To disable plug-ins, visit the Plug-ins page at <chrome://plugins/>. Find the plug-in that you'd like to disable and click Disable. You can also reenable disabled plug-ins on this page.

To Turn off Java in Safari In Safari, choose Safari > Preferences or press Command-comma (?-,)

Click "Security".

Uncheck (deselect) "Enable Java".

Close the Safari preferences window.

For whitehats Here is the [Exploit](#)

chillaxbro - August 29, 2012, 11:09 am

What can this do to me if im using a mac

Antigen - August 29, 2012, 11:10 am

@NEZOS:Mac gets affected too,Dude Java is platform independent!!!(Want a proof see the news!!!)

Super Effective - August 29, 2012, 11:15 am

(Aug 29, 2012 11:09 AM)NEZOS Wrote: [\[CITE\]](#) What can this do to me if im using a mac
You are ignorant if you think viruses don't effect Mac's. There are and have been RAT's for every platform for a long time now. The purpose of professionally made JDB's is to distinguish the users OS and distribute the correct version of the virus. One for Windows, Linux, and Mac.

Don't be as ignorant as the rest of the Mac population and take some initiative.

chillaxbro - August 29, 2012, 12:04 pm

(Aug 29, 2012 11:15 AM)Super Effective Wrote: [\[CITE\]](#) You are ignorant if you think viruses don't effect Mac's. There are and have been RAT's for every platform for a long time now. The purpose of professionally made JDB's is to distinguish the users OS and distribute the correct version of the virus. One for Windows, Linux, and Mac.

Don't be as ignorant as the rest of the Mac population and take some initiative.

Dude what the fuck??? Did i say that nothing will happen to me? I just asked what would happen

?Fear - August 29, 2012, 12:22 pm

Is this a silent JDB?

Thanks for share, btw.

E36 - August 29, 2012, 12:26 pm

I just don't even have java installed. I don't need it anyway.

Inmodwetrust - August 29, 2012, 12:28 pm

Thanks for the head's up, It's much appreciated.

Moneytize - August 29, 2012, 12:31 pm

This made me laugh cuz it isnt Oday anymore lulz....

Antigen - August 29, 2012, 12:36 pm

@?Inmodwetrust™, Ozuru : You are welcome dudes,

@Dude: I know but until this vulnerability get a name every body have to call it Oday most likely.

tux1 - August 29, 2012, 1:44 pm

(Aug 29, 2012 12:22 PM)Ozuru Wrote: [\[CITE\]](#) Is this a silent JDB?

Thanks for share, btw.

Yes it is silent. This message is long enough.

Super Effective - August 29, 2012, 2:42 pm

(Aug 29, 2012 12:04 PM)NEZOS Wrote: [\[CITE\]](#) Dude what the fuck??? Did i say that nothing will happen to me? I just asked what would happen

I do admit I read your post wrong, but my post still answers your question (in an admittedly mean way).

If you run Java, you are at risk at all the basic things that come with Java Drivebys. Just disable it and you should be fine. There is nothing special that happens with Macs.

7ewis - August 29, 2012, 2:54 pm

Is the site safe to visit now? Chrome told me it was infected with malware, so I'm on my iPod touch now.

Don't want to get into the arrogant 'I don't get any viruses' sorta thing either, but I'm running Ubuntu 12.04, what could it do?

Also, I think we need a guide on how to remove this malware from the HF staff! I probably don't know what in talking about so can someone explain :p

Super Effective - August 29, 2012, 2:59 pm

(Aug 29, 2012 02:54 PM)7ewis Wrote: [\[CITE\]](#) Is the site safe to visit now? Chrome told me it was infected with malware, so I'm on my iPod touch now.

Don't want to get into the arrogant 'I don't get any viruses' sorta thing either, but I'm running Ubuntu 12.04, what could it do?

Also, I think we need a guide on how to remove this malware from the HF staff! I probably don't know what in talking about so can someone explain :p

I'll say it again, along with all the other threads posted here. Disable/Uninstall Java until it's fixed. I'm running Debian and never had Java in the first place, so I feel pretty safe.

r0n1n - August 29, 2012, 3:00 pm

Can NoScript prevent this exploit, or there's no other way except disabling java totally?

7ewis - August 29, 2012, 3:03 pm

(Aug 29, 2012 02:59 PM)Super Effective Wrote: [\[CITE\]](#) I'll say it again, along with all the other threads posted here. Disable/Uninstall Java until it's fixed. I'm running Debian and never had Java in the first place, so I feel pretty safe.

I don't really know what the exploit can do, but I guess if your already infected.. Which we could be because we visit HF, uninstalling Java wouldn't cure your system would it?

I read this somewhere:

"it works against a fully patched Windows 7 SP1 with Java 7 Update 6, Mozilla Firefox on Ubuntu Linux 10.04, Internet Explorer / Mozilla Firefox / Chrome on Windows XP, Internet Explorer / Mozilla Firefox on Windows Vista and Windows 7, and Safari on OS X 10.7.4."

(Sorry, it's hard to reference on iPod). Does that mean 12.04 and Chrome would mean I'm protected?

Obviously, I'll still disable it.

Super Effective - August 29, 2012, 3:17 pm

(Aug 29, 2012 03:03 PM)7ewis Wrote: [\[CITE\]](#) I don't really know what the exploit can do, but I guess if your already infected.. Which we could be because we visit HF, uninstalling Java wouldn't cure your system would it?

HackForums is flagged because some idiot got banned and decided to make tons of accounts linking to a JDB using the exploit. If you didn't click any links you're fine.

Just disable Java and continue browsing. I sometimes wonder why people have Java in the first place, but that's a discussion for another time.