New Java Attack Rolled into Exploit Packs

March 27, 2012 51 Comments

If your computer is running **Java** and you have not updated to the latest version, you may be asking for trouble: A powerful exploit that takes advantage of a newly-disclosed security hole in Java has been rolled into automated exploit kits and is rapidly increasing the success rates of these tools in attacking vulnerable Internet users.

The exploit targets a bug in Java (CVE-20120-0507) that effectively allows the bypassing of Java's sandbox, a mechanism built into the ubiquitous software that is designed partly to blunt attacks from malicious code. **Microsoft's Malware Protection Center** warned last week that new malware samples were surfacing which proved highly effective at exploiting the flaw. Microsoft says the samples it saw loaded the ZeuS Trojan, but thieves can use such attacks to install malware of their choosing.

According to posts on several underground carding forums, the exploit has now been automatically rolled out to miscreants armed with BlackHole, by far the most widely used exploit pack. An exploit pack is a software toolkit that gets injected into hacked or malicious sites, allowing the attacker to foist a kitchen sink full of browser exploits on visitors. Those visiting such sites with outdated browser plugins may have malware silently installed, and Java is almost universally the most successful method of compromise across all exploit kits.

According to software giant **Oracle**, Java is deployed across *more than 3 billion systems worldwide*. But the truth is that many people who have this powerful program installed simply do not need it, or only need it for very specific uses. I've repeatedly encouraged readers to uninstall this program, not only because of the constant updating it requires, but also because there seem to be a never-ending supply of new exploits available for recently-patched or undocumented vulnerabilities in the program.

Case in point: On at least two Underweb forums where I regularly lurk, there are discussions among several core members about the sale and availability of an exploit for an as-yet unpatched critical flaw in Java. I have not seen firsthand evidence that proves this 0day exploit exists, but it appears that money is changing hands for said code.

If you do not need Java, junk it; you can always re-install it later if you need to. If you need Java for a specific Web site, I would suggest a two-browser approach. If you normally browse the Web with **Firefox**, for example, consider disabling the Java plugin in Firefox (from the Add-ons menu, click Plugins and then disable anything Java related, and restart the browser), and then using an alternative browser (**Chrome**, **IE9**, **Safari**, etc.) with Java enabled to browse only the site that requires it.

The Java latest versions (which patch the CVE-2012-0507 hole) are *Java Version 6 Update 31*, or *Java 7 Update 3*, released on Feb. 15, 2012. Please note that if you disable the Java plugin from a browser, the next time you update the program, you may need to disable it again, as Java tends to re-enable itself with every security update.

Update, March 28, 3:48 p.m. ET: Marcus Carey, a security researcher at Rapid7, adds a bit more perspective on the severity of the situation with this exploit. He estimates that *upwards of 60 to 80 percent of users probably are not yet patched against this flaw*. Here's what he wrote:

> Anytime an exploit, such as one for CVE-2012-0507, is added to mass exploit kits it goes from being a "hypothetical risk" to becoming a *real* risk. This particular exploit can be found in the widely used BlackHole Exploit kit.
>
> Based on the Java patching habits of 28 million unique Internet users, Rapid7 estimates that 60-80% of computers running Java are vulnerable to this attack today.
>
> Looking long term, upwards of 60% of Java installations are never up to the current patch level. Since so many computers aren't updated, even older exploits can be used to compromise victims.
>
> Rapid7 researched the typical patch cycle for Java and identified a telling pattern of behavior. We found that during the first month after a Java patch is released, adoption is less than 10%. After 2 months, approximately 20% have applied patches and after 3 months, we found that more than 30% are patched. We determined that the highest patch rate last year was 38% with Java Version 6 Update 26 3 months after its release.

Since this is only about a month since the patch was released (February 15), it's likely that only approximately 10% of users have applied the patch.

This entry was posted on Tuesday 27th of March 2012 10:11 AM

A LITTLE SUNSHINE | LATEST WARNINGS | TIME TO PATCH

BLACKHOLE | CVE-2012-0507 | EXPLOIT KIT | EXPLOIT PACK | JAVA | ORACLE

51 thoughts on "New Java Attack Rolled into Exploit Packs"

BruceVA

March 27, 2012

Your point of 2 browsers is interesting. It seems what we really need is to have browsers allow multiple, independent installations of a single browser on a single machine, so that each could be configured differently for different purposes. I wonder how we could get the browser makers to listen.

TJD

-

March 27, 2012

At least one major browser allows you to have multiple "profiles" on each machine. Now if only we could get browser users to listen.

Neej

-

March 29, 2012

Yeah as mentioned Firefox allows profiles although TBH they are somewhat harder to implement to my satisfaction than just a few clicks. It should be easier so more users can use them.

You can also install the portable versions of browsers and optionally sandbox these installs or your normal installation.

Pity FF is so crap compared to chrome which doesnt allow profiles heh

Fred

-

March 30, 2012

Well, Chrome does allow profiles… indirectly. 😀

You could always create a script/starter which symlinks (dunno what it's called on windows) to different settings-folders before starting Chrome/Chromium itself..

At least on Linux this is possible, and I use it myself.

- david gunnells

-

March 31, 2012

Chrome allows profiles directly. - http://support.google.com/chrome/bin/answer.py?hl=en&answer=2364824

As for running java in chrome: at least with newer versions of chrome (I'm using chromium 20 and chrome 19), it will prompt you to allow java to run, so these exploits would most likely fail unless 1) you allowed them to run by clicking one of the buttons in the yellow infobar that pops up or 2) the exploit was running on a site that'd you'd already previously whitelisted.

I See What You Did There

March 27, 2012

Here, let me fix that first sentence for you

"If your computer is running Java, you may be asking for trouble."

Cheers

Patrick

-

March 28, 2012

why not make it:
"If your computer is running, you may be asking for trouble."?

stupid java bashing

John S

March 27, 2012

I have disabled Java, but when I try to remove it, I get error code 1606?

Any ideas on how to proceed?

Thanks?

uzzi

-

March 27, 2012

Google knows! (search for: Error 1606 uninstall Java)

satrow

March 27, 2012

Java and other plugins can be disabled/enabled 'on the fly' in Firefox (and other browsers?). Is restarting Firefox really necessary after making such a change (I know it is for the majority of Add-ons).

- BrianKrebs Post author

-

March 27, 2012

Not sure. But I can send you a few links to some exploit kits if you want to test out my theory firsthand 🙂

satrow

-

March 27, 2012

Hmm, considering it … 😉

JPierini

-

March 29, 2012

Yes please. I would love to see how they would interact with some of my client's desktop images. It would make a powerful argument for reviewing the hardening practices.

- Nick Braak

-

March 28, 2012

For firefox I heartily recommend this extension:

- https://addons.mozilla.org/en-US/firefox/addon/quickjava/

It allows quick enable and disable of Java, Javascript, Flash, Silverlight, Images, Stylesheets and Proxy from the Statusbar and/or Toolbar without having to open any dialogs.

In firefox I leave Java toggled off all the time, enabling only for gov type sites, court case access etc.

Kafeine

March 27, 2012

Here you can see this in action :
http://www.youtube.com/watch?v=2MZxjDVq_bo
Here the VT analysis of the Jar file used on BH EK for this exploit
https://www.virustotal.com/file/69e5b37dbfe4cdf35a5908a7831099726867aa871fdc6abb3468ae397106fdf1/analysis/

Charles Green

March 27, 2012

I find it interesting that on this page my Chrome browser reports that it has blocked JavaScript; I wonder what part of this page is trying to invoke it…

- BrianKrebs Post author

-

March 27, 2012

Charles — both of the ads that run at the top of my blog have flash in them, and script blockers like noscript block flash by default. I can assure you that these ads are malware free, if you'd like to unblock them and support my site. thanks.

Charles Green

-

March 27, 2012

Brian,

Thanks for the response. I still get the JavaScript gripe even though I am not blocking plugins (and can see your ads). This is using Chrome's built-in preferences selection for blocking JavaScript, not a browser add-on such as 'noscript'.

So it's apparently something else about your "don't use Java unless you have to" page which uses JavaScript… 🙂

-Charles

- Brian Krebs

-

March 27, 2012

There are a few other things that ask for Javascript on the site, like the Topsy (Twitter counter), Google Analytics, and the AdThis feature that makes it easy to subscribe to RSS feeds, etc.

Patrick

-

March 28, 2012

you mix up java an java script.
two things that have installation- and security-wise close to nothing in common.

I also think that your advice to "uninstall java" is far off.
At best I'd advice people to uninstall the java *plugin*

In my eyes you're loosing credibility here…

and btw: bashing java and having flash on the site is also a bit of a thing.

best regards
patrick

uzzi

-

March 27, 2012

Sry, Brian, no way I enable flash… but I buy the DVD, the stickers, the cap, the key ring and the mug and the posters (the Who-is-who-of-cybercrooks and Short-history-of- cybercrime are my favorites). */hugs*

- Brian Krebs

-

March 27, 2012

Hmmm. Mugs, keychains….by George you may be onto something there!

Patrick S.

-

March 28, 2012

Dang, I was all excited to hit the store and get my Krebs gear. No such thing, apparently.

JCitizen

-

March 30, 2012

Me too! 😀

Krazytib
March 27, 2012
Are there any sites out there that you can safely test your browser security against the latest exploits to see if your vulnerable or not?

You missed a bit
-
March 27, 2012
Who would trust it?

- AlphaCentauri
-
March 28, 2012
The only way to know you are protected with 100% certainty is to have an AV program that is 100% effective. As Brian mentioned, the bad guys have a lot of incentive to find new vulnerabilities before your AV company does.

R B
March 27, 2012
What is a “publicly undocumented” vulnerability?

YNK
-
March 27, 2012
I’d define that as “any vulnerability without a CVE number.”

Barry
March 27, 2012
I keep Java uninstalled on my XP Pro machine running Windows SteadyState. If I ever need it, I just do an install from an installation package kept on my desktop, when I’m done I reboot to have a clean machine again. Over the last 5 months I have needed Java very few times

SeymourB
-
March 27, 2012
I do something similar, except I run a Windows XP virtual machine. When I want to restore the VM to an earlier state I just overwrite the HD image file from a backup I make periodically.

Windows 7 Pro/Ent/Ult includes a license for XP Mode, it’s silly not to take advantage of it, even if just for playing in a sandbox.

uzzi
-
March 27, 2012
[JFTR: “Sandboxie runs your programs in an isolated space which prevents them from making permanent changes to other programs and data in your computer.” (sandboxie.com)]

Jane

-

March 28, 2012

Where I work, we're not allowed to use / install XP Mode because IT can't push updates to the XP image the way they can to our actual machines.

Omer bauer

March 27, 2012

Bran……..Two years ago you said to dump Java if you don't need it…and I did. I haven't seen any difference in my computer between Vista and now Windows 7. Thank you for the advice.
Omer Bauer.. A loyal follawer

67GTV

-

March 29, 2012

"Bran is often used to enrich breads (notably muffins) and breakfast cereals, especially for the benefit of those wishing to increase their intake of dietary fiber."
- http://en.wikipedia.org/wiki/Bran

Both Brian and Bran help to keep you 'regular'. 😉

JCitizen

-

March 30, 2012

Well at least that is better than calling him Brain, like I did with one embarrassing type once! :8}

mutifo

March 28, 2012

Security by Isolation is a good approach.
Qubes is an open source operating system designed to provide strong security for desktop computing.
http://qubes-os.org/Home.html

asdfasddfdf

March 28, 2012

The downside of the two browser approach is that it doesn't prevent the 'safe' browser from asking if you want to open a .jnlp file which will invoke Java Web Start. It's also a good idea to remove the file association for .jnlp.

emil

March 28, 2012

sorry guys, but i use firefox with request policy and no script. so no "support" from me. but i like to minimize cross domain requests. (why cant sites at least have there css files on the same domain?!) . i have java installed. need it, want it. but have the browser plugin's all disabled. (multiple java versions here). i think ff blocks java from activating the plugin or am i wrong?

lg

emil

satrow

-

March 28, 2012

FX enables the Java plugin by default (as do all browsers that I've checked recently), you need to disable it via Tools > Add-ons > Plugins; restart FX to be sure that it's disabled (though I think it's safe to enable/disable it 'on the fly').

Charles

-

April 3, 2012

emil, larger sites put CSS on other domains for CDN and load balancing management. Also, I'm seeing some confusion among some readers about the difference between JavaScript and Java. These are two entirely distinct languages/runtimes. JavaScript is embedded in all modern browsers and is actually necessary to run many modern websites. Turning it off, in my opinion, is the same as simply not using the web for anything beyond casual reading.

Java, on the other hand, is an object oriented language similar to C++ that runs in something called virtual machines. VMs execute the Java programs. Disabling Java is a personal choice, but I prefer to 1) visit sites I trust, and I never click links in emails and 2) Always update my Java instances, which is easy to do on a mac. Removing Java isn't an option, as I am a developer and need it for my work.

There will always be both JavaScript and Java-based exploits. The best prevention is to rely on sites you trust, and never click links you get an email, for any reason, even if the email is from a friend. If somebody sends you an "interesting" link, at least put the first part of the address in google and see if it comes up as part of a known phishing exploit. Also, there is a proxy malware detector called DNSCrypt from OpenDNS that can help prevent proxy attacks.

Philip

March 28, 2012

The exploits for CVE2012-0507 have been in the wild for at least three weeks now. If you are still running a vulnerable Java, and have it accessible through your browser on Windows, chances are high and increasing that you will be "had". Today, we encountered these sploits on web sites covering so diverse topics as Food&Wine, Excel Help, and Perfume .. all of which are frequented by "casual surfers". The EXEs that are pushed by the sploit come back as 0/43 or 1/43 on Virustotal, which means that your AntiVirus WONT HELP. Take Brian's advice seriously: Uninstall Java, or patch it.

k

-

April 4, 2012

actually, what vtotal tells you is that you have found some malware. it doesn't give you an accurate evaluation of anti-malware performance. that statement is ignorant and bogus.

Karl

March 28, 2012

I remove malware all day long from computers that have every antivirus and antimalware program on the planet and have come to the conclusion that behavior is 99% of the problem. If you get tricked into clicking on the wrong thing your AV program creates an exception and now you have a fake antivirus program running on your computer.

Eddie

March 29, 2012

While this article is great for awareness. It really promotes more fear mongering that java is a very very bad thing to have. This CVE may bypass sandboxing but you are forgetting a few things to tell your readers. While it may be easy to write and say patch now especially to corporations patching to the latest versions isn't such an easy task. Instead mitigation techniques should be touted such as enabling perimiter security on your firewall to allow java to only work with known trusted websites. Don't forget letting users run without elevated privilages will limit some of the damage blackhole exploits can do. There are other layers. Antivirus signatures updated to detect the problem and IDS systems such as Snort or Dell secureworks that monitor network traffic based intrusions. Not saying you should run unpatched. Just stating that some corporations just can't jump ship and hop from one version to another because of dependent applications that may require specific versions of Java. While patching is one thing taking an onion and requiring people to peel back the layers should be the first tactical approach to any security situation.

TheNovaGp

March 30, 2012

I dont have the lates java version, thats is a trouble? i need delete the java i have?

Orlando

March 30, 2012

Every time you post about Java and suggest it might be uninstalled as unecessary, I reconsider my own needs.

Until now, I have kept it because the Open Source software I used to make backups is written in Java. I've finally an found alternative which does not require Java and have uninstalled it.

I was also anxious that removing Java might break LibreOffice for me but as far as I can tell, it is only the database component and the wizards in the word processor that are affected.

Thanks for your blog
Best Wishes,
Orlando.

Lenise

March 31, 2012

Notwithstanding any required business use. You can have the full functionality of 98 of the web not having Java installed or at least disabled.

If for some reason you require Java Runtime b/c you use Java coded programs (Open Office, Jdownloader) You can manually delete the plugins to keep all your browsers Java free but still retain the use any Java based program.

Of course you have to do this process again if you update Java. I written down what I need to delete so I can do the process in 5 mins or less.

C:\Program Files (x86)\Java\jre7\bin\new_plugin\npdeployJava1.dll

C:\Program Files (x86)\Java\jre7\bin\new_plugin\npjp2.dll

C:\Program Files (x86)\Java\jre7\bin\ssv.dll

C:\Program Files (x86)\Java\jre7\bin\wsdetect.dll

C:\Program Files (x86)\Java\jre7\bin\npjpi70_01.dll

C:\Program Files (x86)\Java\jre7\bin\jp2ssv.dll

C:\Program Files (x86)\Java\jre7\bin\npoji610.dll

After you do that, restart your browser and check to see if Java is still there by going into the browser GUI or go to

http://www.mozilla.org/en-US/plugincheck/

Weng Fu

April 1, 2012

The Javascript can be disabled using the menu stick action. If you disable Javascript this problem does not have chance of happen.

alex

April 8, 2012

And this is why I don't have the Java plugin installed.

Still, in Firefox removing this until you're patched is easy: Tools > Add-ons > go to extensions tab > disable Java

Online Tech Support

April 17, 2012

Thanks for inform..I have disabled java in my system. how can I get this problem..

Comments are closed.