

Java vulnerability for 1.7.10 and below

Last Updated: Wed Jan 16 10:46AM PST

Overview

A new critical vulnerability has been discovered in Java 1.7.x. Your computer could be instantly compromised without your knowledge if you visit a website with hostile Java code; this is known as a drive-by-download. There are reports that this vulnerability is now being used to actively attack computers on the Internet. The only protection against this serious attack is to update or disable your Java software.

Status and Recommendation

First visit the LBL Browsercheck site which will verify whether you need to update:

<http://go.lbl.gov/browsercheck>

If you have Java 1.7.x, Oracle has released Java version 1.7.11 for this vulnerability, you should install it immediately. At this time, the latest version of Java 1.6.x (1.6.38 on Windows) is secure. The latest version of Java 1.6 on Mac is secure against this vulnerability. When in doubt, Browsercheck is the best tool we know of to determine if a given version is safe.

Download 1.7.11 at <http://www.java.com/getjava/>

Once it has been installed, you should verify all browser plugins are updated by visiting Browsercheck again:

<http://go.lbl.gov/browsercheck>

Note: If you have previously disabled Java Plugin in the browser, you will need to manually re-enable it after installing this release. In Firefox, you can do this in the Add Ons -> Plugin screen. In Internet Explorer, this functionality is located in Tools -> Manage Add-ons.

If you have disabled Java in the Java Control Panel, you will need to manually re-enable it after installing this release. You can find the check box in the Security tab of the Java Control Panel.

Questions?

Please contact the helpdesk at x4357 or help@lbl.gov for general support questions or assistance with updating Java. Contact security@lbl.gov with specific security concerns related to this vulnerability.

References

- <http://www.oracle.com/technetwork/java/javase/7u11-relnotes-1896856.html>
- <http://www.kb.cert.org/vuls/id/625617>
- https://threatpost.com/en_us/blogs/nasty-new-java-zero-day-found-exploit-kits-already-have-it-011013
- <http://labs.alienvault.com/labs/index.php/2013/new-year-new-java-zero-day/>
- <http://krebsonsecurity.com/2013/01/zero-day-java-exploit-debuts-in-crimeware/>
- <http://malware.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html>

Alternative - Disable Java

While this is not yet recommended, some may choose to implement this precaution now. The repercussions of disabling Java vary widely. Some people use web applications that require Java, so disabling it may render these applications inoperable. Others will find that disabling Java doesn't affect their daily work and may choose to leave it disabled for added protection.

- Instructions to disable Java on many browser and platforms are [here](#)
- Detailed OSX specific instructions are [here](#)

Gory Details

- Exploit code is [here](#)