CERT Advisory CA-1996-07 Weaknesses in Java Bytecode Verifier

Original issue date: March 29, 1996
Last revised: September 24, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of weaknesses in the bytecode verifier portion of Sun Microsystems' Java Development Kit (JDK) versions 1.0 and 1.0.1. The JDK is built into Netscape Navigator 2.0 and 2.01. We have not received reports of the exploitation of this vulnerability.

When applets written with malicious intent are viewed, those applets can perform any operation that the legitimate user can perform on the machine running the browser. For example, a maliciously written applet could remove files from the machine on which the browser is running--but only if the legitimate user could also.

Problem applets have to be specifically written with malicious intent, and users are at risk only when connecting to "untrusted" web pages. If you use Java-enabled products on a closed network or browse the World Wide Web but never connect to "untrusted" web pages, you are not affected.

The CERT staff recommends disabling Java in Netscape Navigator and not using Sun's appletviewer to browse applets from untrusted sources until patches are available from these vendors. We further recommend upgrading to Netscape 2.02 but still disabling Java and JavaScript if you don't need these programs.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The Java Programming Language is designed to allow an executable computer program, called an applet, to be attached to a page viewable by a World Wide Web browser. When a user browsing the Web visits that page, the applet is automatically downloaded onto the user's machine and executed, but only if Java is enabled.

It is possible for an applet to generate and execute raw machine code on the machine where the browser is running. This means that a maliciously written applet can perform any action that the legitimate user can perform; for example, an applet can read, delete, or change files that the user owns. Because applets are loaded and run automatically as a side-effect of visiting a Web page, someone could "booby-trap" their Web page and compromise the machine of anyone visiting the page. This is the problem described in the Wall Street Journal on March 26, 1996 ("Researchers Find Big Security Flaw in Java Language," by Don Clark).

Note: The security enhancements announced by Sun Microsystems in JDK version 1.0.1 and by Netscape Communications in Netscape Navigator version 2.01 do *not* fix this flaw.

II. Impact

If Java is enabled and a Web page containing a maliciously written applet is viewed by any of the vulnerable browsers or Sun's appletviewer, that applet can perform any operation that the legitimate user can perform. For example, the applet could read, delete, or in other ways corrupt the user's files and any other files the user has access to, such as /etc/passwd.

III. Solution

We recommend obtaining vendor patches as soon as they become available. Until you can install the patches, we urge you to apply the workarounds described below.

A. Java Development Kit users

Sun reports that source-level fixes will be supplied to source licensees in the next few days. The fixes will also be included in the next JDK version, v1.0.2, which will be released within the next several weeks.

The JDK itself is a development kit, and it can safely be used to develop applets and applications. If you choose to use the appletviewer as a rudimentary browser, do not use it to browse applets from untrusted sources until you have installed the v1.0.2 browser.

B. Netscape users

Upgrade to Netscape version 2.02, which addresses the Java Bytecode Verifier problems discussed in the advisory.

Until you can do so, if you use Netscape 2.0 or 2.01, disable Java using the "Security Preferences" dialog box. You do not need to disable JavaScript as part of this workaround.

After you update to version 2.02, you should still disable Java and JavaScript if these programs are not being used. (This also applies to Netscape Version 3.0b4.) Note that in order to display Netscape's home page, you must have JavaScript enabled.

For the latest news about fixes for Netscape Navigator, consult the following for details:

http://home.netscape.com/

Netscape 2.02 and additional information about it are available from

http://home.netscape.com/eng/mozilla/2.02/relnotes/

IV. Information for HotJava (alpha3) users

Sun Microsystems has provided the following information for users of HotJava (alpha3).

> Sun made available last year a demonstration version of a browser called "HotJava." That version (alpha3) is proof-of-concept software only, not a product. HotJava (alpha3) uses an entirely different security architecture from JDK 1.0 or JDK 1.0.1. It will not be tested for any reported security vulnerabilities that it might be susceptible to, and Sun neither supports it nor recommends its use as a primary browser. When HotJava is released as a product, it will be based on an up-to-date version of the JDK and fully supported.

V. Information for Macintosh users

Macintosh version 2.01 does not support Java, so there is nothing to disable as part of the solution to the problems described in this advisory.

The CERT Coordination Center thanks Drew Dean, Ed Felten, and Dan Wallach of Princeton University for providing information for this advisory. We thank Netscape Communications Corporation and Sun Microsystems, Inc. for their response to this problem.

Revision History

```
Sep. 24, 1997 Updated copyright statement
Aug. 30, 1996 Information previously in the README was inserted into
              the advisory.
June 26, 1996 Introduction - added a note about Netscape 2.02.
              Sec.III.B - added a pointer to Netscape 2.02 and a
              recommendation about disabling Java and JavaScript.
Apr. 1, 1996 Sec. III.B - added a note about viewing
             Netscape's home page.
             Sec. V - added this section for Macintosh users.
```