CERT Advisory CA-2000-15 Netscape Allows Java Applets to Read Protected Resources

Original release date: August 10, 2000
Source: CERT/CC

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

Systems Affected

- Systems running Netscape Communicator version 4.04 through 4.74 with Java enabled. Netscape 6 is unaffected by this problem.

Overview

Netscape Communicator and Navigator ship with Java classes that allow an unsigned Java applet to access local and remote resources in violation of the security policies for applets.

I. Description

Failures in the netscape.net package permit a Java applet to read files from the local file system by opening a connection to a URL using the "file" protocol. For example, by opening a connection to "file:///C:/somefile.txt" an intruder can read the contents of that file.

Additionally, it is possible to use this technique to open connections to resources using other types of protocols; that is, it is possible to open a connection to "http," "https," "ftp," and other types of URLs using this vulnerability.

By then using ordinary techniques, a malicious Java applet that exploits this vulnerability could subsequently send the contents of the file (or other resource) to the web server from which the applet originated.

An exploit using this technique causes the victim to establish a connection to the malicious web server (as opposed to the intruder establishing a connection to the victim). Thus typical firewall configurations fail to stop an attack of this type.

A tool written by Dan Brumleve dubbed "Brown Orifice" demonstrates this vulnerability. Brown Orifice implements an HTTP server (web server) as a Java applet and listens for connections to the victim's machine. In conjunction with the Netscape vulnerability, Brown Orifice essentially turns a web browser into a web server and allows any machine on the Internet to browse the victim's local file system. Typical firewall configurations stop this type of attack, but as noted above, they do not stop simple variations of this attack.

This vulnerability is the result of an implementation error in the JRE that comes with the Netscape brower, not an architectural problem in the Java security model.

This problem has been widely discussed in various forums on the Internet. More information is available at

> http://www.securityfocus.com/bid/1546
> http://www.nipc.gov/warnings/assessments/2000/assess00-052.htm
> http://xforce.iss.net/alerts/advise58.php
> http://www.brumleve.com/BrownOrifice (Note that this site contains a demonstration of the vulnerability which could expose your files to intruders.)

As of the writing of this document, we have not received any reports indicating exploitation of this vulnerability outside of the context of obtaining it from the Brown Orifice web site. Note that running Brown Orifice allows anyone, not just the administrators of the Brown Orifice web site, to read files on your system. The Brown Orifice web site publishes the IP address of systems running Brown Orifice, and we have received reports of third parties attempting to read files from a system identified on the Brown Orifice web site. Furthermore, if you have extended any file-reading privileges to anyone who has run Brown Orifice, your files can be read by anyone on the Internet (subject to controls imposed by your router and firewall.)

II. Impact

Intruders who can entice you into running a malicious Java applet can read any file that you can read on your local or network file system. Additionally, the contents of URLs located behind a firewall can be exposed.

III. Solution

Organizations should weigh the risks presented by this vulnerability against their need to run Java applets. At the present time, an effective solution is to disable Java in Netscape. Historically, vulnerabilities of this type have *not* been widely exploited; however this is not an indication that they can't be, or that targeted attacks are not effective and possible.

For organizations that have a need to run Java applets under their own control (that is, in situations where the HTML page referencing the applet is under their control), an alternate solution is to install a Java Runtime Environment Plugin available from Sun Microsystems. More information and pointers to downloadable software is available at

> http://java.sun.com/products/plugin/index.html

To use this plugin effectively requires the use of a tool to convert HTML pages to use a different tag. Information about Sun's HTML Converter Software is also available on
this page. This tool will rewrite HTML pages so that applets referenced in the page will run in the JRE provided by the plugin.

To achieve protection from the resource reading vulnerability using this tool requires you to disable Java in the Netscape browser. The HTML Converter software will modify HTML pages to use an <EMBED> tag instead of an <APPLET>. The JRE plugin software recognizes the <EMBED> tag, and applets will then run within the new JRE plugin, instead of the default JRE provided by Netscape.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A. Vendor Information

AOL Corporate Communications

Netscape takes all security issues very seriously, and we are working to quickly evaluate and address this concern. If the reports are accurate, we plan to make a patch available, but in the interim, users can protect themselves by simply turning off Java.

Users can also visit
http://www.netscape.com/security to get the mostup to date information on a patch, and its availability.

Sun Microsystems and Netscape

Sun is working with Netscape to deliver a new version of Navigator and Communicator that will fix this problem.

Microsoft

Brown Orifice does not exploit any vulnerabilities in Microsoft Products.

The CERT Coordination Center thanks Elias Levy, CTO of SecurityFocus.com, and Sun Microsystems and AOL/Netscape for their input and assistance in the construction of this advisory.

Author:
Shawn Hernan

Revision History

```
August 10, 2000:  Initial release
```