

Securiteam: [NEWS] Java Web Start Argument Injection Vulnerability (property)

[NEWS] Java Web Start Argument Injection Vulnerability (property)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0094.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/22/05

To: list@securiteam.com

Date: 22 Mar 2005 10:52:38 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Java Web Start Argument Injection Vulnerability (property)

SUMMARY

<<http://java.sun.com/products/javawebstart/>> Java Web Start is a technology for easy client-side deployment of Java applications. "Using Java Web Start technology, standalone Java software applications can be deployed with a single click over the network".

A vulnerability has been found in Java Web Start system 'property' tag, allowing malicious user to pass command line arguments to the Java virtual machine(JVM). Passed arguments could be used to tweak JVM's system settings to disable the Java "sandbox" and compromise the system.

DETAILS

Vulnerable Systems:

- * Java Web Start delivered with Java2 Standard Edition(J2SE) versions 1.4.2 to 1.4.2_07

Immune Systems:

- * Java Web Start delivered with J2SE version 5.0
- * Java Web Start delivered with J2SE versions prior to 1.4.2

[NEWS] Java Web Start Argument Injection Vulnerability (property)

Securiteam: [NEWS] Java Web Start Argument Injection Vulnerability (property)

The `<property>` tag in a Java Network Launching Protocol (JNLP) file can be used to define Java system properties. System properties are key–value pairs which usually store attributes of the current working environment, e.g. "java.home" containing the Java installation path and "java.version" containing its version. Due to the nature of some of the system properties, setting their values in JNLP files is restricted.

A few system properties are considered "secure" and if defined in a JNLP file, they are passed to the Java executable (javaw.exe) via the `-Dproperty=value` command line argument. However, a malicious user can use this feature to inject extra command line arguments to the Java executable.

For instance, a JNLP file can contain this property tag:

```
<property name="sun.java2d.noddraw" value="true HELLO" />
```

The property "sun.java2d.noddraw" is considered secure by Web Start, so it is accepted and the startup command for the application is something like this:

```
javaw.exe -Dsun.java2d.noddraw=true HELLO (other args) your.application
```

This would produce a Web Start error message saying the main class can't be found, as javaw.exe interprets "HELLO" as the main class name instead of "your.application". The problem is that Web Start fails to use quote symbols around the property argument.

To exploit the flaw, an attacker can pass command line arguments affecting the Java security policies. Normally an unsigned, untrusted Java applet operates inside a "sandbox" and can't e.g. access local files. By exploiting this flaw, the default "sandbox" security policy can be overridden with an arbitrary policy file hosted on the attacker's web server. The new policy can grant full permissions to the application, which could then e.g. read or write arbitrary files on the victim system, or download and launch viruses, keyloggers or other malware. The attacker may set up a JNLP file on a web server so that it will be launched without further user interaction when the victim visits the site, e.g. with the IFRAME tag.

As the application is made in Java, the same exploit can work on any platform supporting Java Web Start. A proof–of–concept exploit was produced which detects the operating system and starts an OS–dependent binary executable when a web page is visited – the same exploit works with Internet Explorer on Windows and Mozilla Firefox and Opera on Linux.

If Internet Explorer is used, the JNLP file is opened automatically without further interaction. Other web browsers may, depending on file type configuration, display a dialog asking whether the file should be opened or saved. Some versions of e.g. Opera require manual configuration in order to open JNLP files.

Securiteam: [NEWS] Java Web Start Argument Injection Vulnerability (property)

In addition to the web browser attack vector, the attacker could replace an existing JNLP file on a web site with a malicious one. Web Start applications can be started from desktop shortcut icons, from the Web Start menu, or from command line. All of these starting methods are suspected to the attack.

Vendor Status:

Sun Microsystems was informed about the problem on September 25, 2004. The issue was fixed in J2SE 1.4.2_07. Sun's advisory can be found at: <<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57740-1>> <http://sunsolve.sun.com/search/document.do?assetkey=1-26-57740-1>

ADDITIONAL INFORMATION

The information has been provided by <mailto:jouko@iki.fi> Jouko Pynnonen.

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.