

Security Warnings Regarding *FastPak for Java*

Terms and Definitions

The following terms and definitions are relevant to this document:

FastPak for Java: *FastPak for Java*, which will also be referenced by its short name, *FastPak*, is the product that is being described in this document.

Software and Computer Systems Company, LLC: **Software and Computer Systems Company, LLC**, which will also be referred to in this document as **SCSC**, is the company that designed and produced *FastPak for Java*.

System: This refers to a specific computer system comprised of a computer, associated peripherals, networking hardware and connections, and an operating system. It does not refer to a networked hub, array, or anything else that may involve more than one, specific computer system.

JNI: The Java native interface. JNI allows programs written in Java to interact with other programs, modules, and libraries written in languages such as “C” and “C++” which produce binaries specific to the hardware platform and its operating system.

Application: An application can refer to *FastPak* itself, or any computer programs written, compiled, and installed on any system. With respect to *FastPak*, a reference to an application will be limited to computer programs compiled into byte codes using a Java compiler, and possibly using JNI components.

Application loader: *FastPak* is a Java based application loader. This means that *FastPak* loads and executes other applications written in the Java language, including those with acceptable JNI components. *FastPak* does not interrogate or make any attempt to prevent an application from running. By default, it does no security checks of any sort. If anyone using *FastPak* executes an application that accesses non-secure data, whether it be via a network connection or other means, then users, developers, and administrators must make concerted efforts to ensure that the data and any other applications running under *FastPak* are not compromised.

Local network: For the purposes of this document, a local network is a secure network that has all its connections limited to other systems on the same network. Many companies implement and maintain such networks by either completely isolating them from external networks, such as the world wide web, or by implementing security devices and software programs that prevent and/or limit systems on the local network from interacting with external networks.

Non-local network: For the purposes of this document, a non-local network is a network which allows a system to make connections with at least one remote system of unknown or unpredictable origin. The unknown or unpredictable remote systems can include, but not be limited to, such things as routers, gateways, and servers. A perfect example of this is the world wide web. If a system exists on a local network (described above) and it

makes connections to an external network using means that are not secure, then the local network itself becomes a non-local network.

Hack, hacked, or hacking: These terms refer to the deliberate alteration of data, either by replacing an existing application that a user is expecting to use with one that has been deliberately modified in one way or another, or by intercepting the flow of data over a network, local on non-local, and altering it in such a way that what the user thinks they are getting has in fact been modified. People that perform hacking are often referred to as “**hackers.**” Some hackers are nothing more than practical jokers, while others are criminals intent on performing acts of theft or vandalism.

Desktop application: For the purposes of this document, a desktop application is an application that has its scope of data and resource (network connections, disk access, etc.) access limited to the system it is running on. **In *FastPak's* case, this will mean *FastPak* itself and all applications it has running underneath it.** In such an environment, network access is limited to *localhost* (the system itself).

Local networked application: For the purposes of this document, a local networked application is an application that interacts with at least one other application on at least one other remote system, but on a network that is secure, and preferably completely isolated from other external networks, such as the world wide web. Many companies implement such networks as company “intranets.”

Non-local networked application: For the purposes of this document, a non-local networked application is an application that interacts with at least one other application on at least one other remote system on a non-local network.

Local work group tool: In terms of *FastPak*, this refers to many instances of *FastPak* working together on a local network as described above.

Controller Thread: *FastPak* can optionally make use of a software component called a *Controller Thread*. The *Controller Thread* allows each instance of *FastPak* installed on each system using the product to allow remote access between itself and other machines on a network, either local or non-local. As installed, this tool does not provide any security of any means. It has, however, been designed in such a way that developers can easily implement their own security procedures, which are discussed in the developers manual for *FastPak*. **Under no circumstances should the *Controller Thread* be exposed to a non-local network without implementing a secure interface!** Additionally, administrators and developers are cautioned about using an unprotected *Controller Thread* from being accessed by users on a local network that may not fully be aware of how the *Controller Thread* works or its potential for misuse, intentional or unintentional.

Remote Loader: *FastPak* can load and execute Java applications in a Java archive format (*jar*) from a remote server via a URL reference. The intent of using the remote loading capability of *FastPak* is **not** to encourage anyone from loading such applications onto a remote server for general use, **particularly on a non-local network,** but rather it's a tool provided to developers to allow users to access applications that are under development using a secure, local network. During the software development process, it's very likely bugs will be discovered. During the testing process, it has historically been the case that developers needed to copy all associated binaries to each individual machine involved in the testing process. *FastPak's* remote loading capability allows the application to be stored on a local web server under a local network without the need to copy and overwrite instances of currently installed applications. A potential security problem can arise if applications are stored on a non-local network and accessed using the remote loading

capabilities of *FastPak*. The only solution to this is to simply prevent personnel using and/or administering *FastPak* from putting applications on a remote server that uses a non-local network.

FastPak and Security

FastPak is not a secure product. It is intended to be used in a controlled environment on a local network. The following security problems may exist with *FastPak* when exposed to a non-local network, but be advised this list likely not a list of all potential security problems:

- **Controller Thread:** The *Controller Thread* is a thread that can allow users on remote systems to execute *FastPak* functions remotely. The *Controller Thread* is only a potential security problem if it is running. If there is no need for it to be running then it should be stopped or never even started (automatic start up of the *Controller Thread* can be configured in *FastPak's* configuration menus). The interface to the *Controller Thread* is not secure. It is the responsibility of those administering and developing for your system(s) to ensure that if the *Controller Thread* is to be used, that its access must be secure. Generally, SCSC recommends that developers create a secure interface to the *Controller Thread*. SCSC does not, and likely will not produce such an interface, but any third party vendors, open source and commercial, are welcome to do so.
- **Remote Loading:** Remote loading can become a security problem in numerous ways, but this section will be limited to the two most likely ways remote loading can present a problem. First, if *FastPak* performs a launch of an application on a remote server and that application itself has been deliberately modified (**hacked**) by people intending to alter the original intent of the program, then the program *FastPak* launches will be what amounts to a fraudulent copy of the original application. Second, if *FastPak* is in the process of downloading an application from a server and the communications channel is intercepted and re-routed, the application that *FastPak* was intending to download and run can be replaced by another program that is likely not what the user was expecting to run. SCSC recommends downloading only from servers within a local network where control of the downloaded application can be properly maintained..
- **Application Problems:** As an application launcher, *FastPak* runs other applications under it. *FastPak* should only be seen as being as secure as its weakest link. As stated previously, *FastPak* will not interfere with any applications or how they are run. This means that if a user is running an application under *FastPak* that uses encrypted and/or secure communication channels to a non-local network, the application will work properly. A potential security problem might exist if the secure application just mentioned is run under *FastPak* simultaneously with another application that accesses and interacts with other systems and applications on a non-local network, or possibly even a local network that has been hacked, without any security whatsoever. In this case, the once secure application should now be seen as being effectively compromised.

If you are working in an environment where security is critical, you may need to analyze in detail whether or not *FastPak* can and should be used in your environment.

DISCLAIMER

Software and Computer Systems Company, LLC, will not accept any liability for any security violations that may be directly or indirectly associated with the use of any of the software supplied with the product *FastPak for Java*. The text above describes what types of security problems may exist if *FastPak* is installed and used, but the text should absolutely, in no circumstances be considered to be complete. Security threats are dynamic and changing every day. It is the duty and responsibility of all those using, installing, developing applications for, and/or administering *FastPak* to see that security is maintained.

Legal Information

All Software and Computer Systems Company, LLC logos are a trademark (TM) of Software and Computer Systems Company, LLC. *JWaveScope* and *FastPak for Java* are trademark (TM) of Software and Computer Systems Company, LLC. All software produced and licensed by Software and Computer Systems Company, LLC is copyright© Software and Computer Systems Company, LLC **2005 - 2007**. The contents of all pages and images contained in this document are copyright© Software and Computer Systems Company, LLC, **2007**,

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and certain other countries. X Windows and the X Window System are trademarks of the X Consortium. UNIX is a registered trademark in the United States and other countries of the X/Open Company, Ltd. Apple Macintosh and OS X are trademarks of Apple Computer, Inc. Novell is a registered trademark of Novell, Inc., and SUSE is a trademark of SUSE LINUX Products GmbH, a Novell business. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Motif is a registered trademark of The Open Group.

Unless explicitly stated, original products and services offered, sold, or licensed to customers by Software and Computer Systems, LLC are the exclusive right of Software and Computer Systems Company, LLC. Clients, users, or interested parties should not assume an affiliation exists between Software and Computer Systems Company, LLC and any of the computer manufacturers, operating system distributors, or other vendors that may be used in the production or completion of a work produced by Software and Computer Systems Company, LLC for a customer or product.