# Security Alert for GlobalSight 8.3

November 22, 2012

This security alert addresses a GlobalSight 8.3 vulnerability to a worm that can affect the JBoss Application Server JMX console. This vulnerability affects GlobalSight 8.3 packages downloaded prior to November 21, 2012 at 12:00 noon Eastern Standard Time.

This original GlobalSight 8.3 enables the JBoss JMX console, which has the vulnerability described here: https://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server . In versions of GlobalSight earlier than 8.3 the JMX console was not enabled, so they do not have this vulnerability.

Remediation steps:

1. Perform the following test (you will run it again later to test that the vulnerability has been fixed):
1. Invoke the JMX console from a web browser. If your GlobalSight URL is http://localhost/globalsight, then your JMX console URL is http://localhost/jmx-console.
2. If the JMX console displays (title: JBoss JMX Agent View <servername>), then your GlobalSight server is vulnerable.
3. Disable the JMX console to eliminate the vulnerability:
1. In the folder <GlobalSight>jbossjboss_serverserverdefaultdeployjmx-console.warWEB-INFclassesorgjbossjmx, rename the adapter folder to adapter.DISABLED (or anything other than adapter).
2. Restart the GlobalSight service.
3. Invoke the JMX console again (or reload the page in the browser). If you get an error (such as HTTP Status 500 or 503), your GlobalSight server is no longer vulnerable. (If the JMX console displays, try reloading.
4. Worm detection and removal: See "Worm detection" and "Worm removal procedure" on https://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server
.

5. Remember to watch for and apply GlobalSight updates as they become available. The GlobalSight 8.3.0.1 is now available on globalsight.com and sourceforge.net.

Additional Information:

1. The GlobalSight 8.3 package with the vulnerability was removed from globalsight.com and sourceforge.net at noon Eastern Standard Time on November 21, 2012. A replacement GlobalSight 8.3 package without the vulnerability will be posted to those sites as soon as it is ready.
2. To determine whether a GlobalSight 8.3 upgrade installer package has the vulnerability, check for the existence of the directory serverGlobalSightjbossjboss_serverserverdefaultdeployjmx-console.warWEB-INFclassesorgjbossjmxadaptor. If this folder exists, the package has the vulnerability. After installing it, follow the remediation steps above.
3. Another way to determine whether a GlobalSight installation has the vulnerability is to check for the existence of the folder <GlobalSight>jbossjboss_serverserverdefaultdeployjmx-console.warWEB-INFclassesorgjbossjmxadapter. If this folder exists, the installation may have the vulnerability. To address it, follow the remediation steps above.

# www.globalsight.com Home Page Problems

There is an intermittent problem with the home page on www.globalsight.com. The web team is looking into it. If you go to www.globalsight.com and get a blank page, please use the following URL to access the site (you should be able to navigate everywhere except possibly the home page): http://www.globalsight.com/index.php?option=com_fireboard&Itemid=101