Java Vulnerability (CVE-2012-4681)
Schneider Electric Critical Power and Cooling Services (CPCS)
Product Statement

Overview:

This bulletin is for Schneider Electric CPCS software products and the Java vulnerability detailed in CVE-2012-4681.

On 28-AUG-2012, US-CERT released a vulnerability advisory regarding the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6, and earlier including Java SE 6. This vulnerability allows the possibility of remote attackers to execute arbitrary code to access restricted classes, and modify private fields in selected areas within the JRE. According to the Oracle advisory, standalone desktop applications are unaffected by this vulnerability.

A review of Schneider Electric CPCS software products was performed to determine if any product offerings contained this vulnerable Java Version.

Products:

Several products use Java as part of their offering. These products include (Java version listed):

- Network Management Card (NMC) Device IP Wizard (Java Version 7)
- Netbotz Advanced View (Java Version 6)
- PowerChute Network Shutdown (Java Version 6)
- PowerChute Business Edition (Java Version 6)
- StruxureWare Data Center Expert (Java Version 6)
- StruxureWare Operations (Java Version 6)

Problem Description:

During the application installation, some Schneider Electric CPCS software products install a private JRE onto a client system. This application only calls the bundled JRE during the application's operation and is not publically available. Specifically, the installed JRE is not available for any users except the specified application, in this case the *Device IP Wizard* for Version 7 JRE. This would classify the product as a standalone application.

Customers utilizing the *Device IP Wizard* would need to make specific system changes to utilize the bundled JRE for other applications. If a customer makes a system path modification and employs the application's private JRE, a customer could potentially open themselves to this vulnerability.

Java Vulnerability (CVE-2012-4681)
Schneider Electric Critical Power and Cooling Services (CPCS)
Product Statement

Products (cont'd):

PowerChute Network Shutdown software allows for the option of using the publicly installed JRE or installing the private JRE during the install process. If users are already using *PowerChute Network Shutdown (PCNS)* with a public JRE version that is vulnerable, they should re-install *PowerChute* (preserve existing settings - similar to an upgrade) and choose the private JRE option **OR** upgrade the public JRE they are using to a patched version.

This will not work for *PowerChute Network Shutdown (PCNS)* 2.2.x - if Java 6 Update 35 and Java 7 Update are both present on the machine the installer will choose Java 6 over Java 7 (limitation of Jexpress installer used in 2.2.x) when *PCNS* is re-installed. To avoid this, users need to stop the *PCNS* service, uninstall Java 6, install Java 7 (patched) and then re-install *PCNS*. This will work for both *PowerChute Network Shutdown* 2.2.x and 3.0.x.

Conclusion:

Customers should be advised to reference US-CERT CVE-2012-4681 for further details. Since these products utilize Java, Schneider Electric CPCS recommends following the vendor's advice and use the latest Java release to avoid this vulnerability with the publically installed JRE.

Further Details:

Specifics related to this vulnerability can be found at the following links:

Oracle (Owner and vendor for the Java code base):
http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

U.S. CERT:
http://www.us-cert.gov/cas/techalerts/TA12-240A.html