CollegeSource Response to Recent Security Alerts (Legacy)

Recently, there have been two security alerts issued by third parties that have raised questions about their impact on CollegeSource products, particularly those that are installed by clients. This is an overview of those alerts and our recommendation to resolving the problems as related to CollegeSource products.

Spring Expression Language Injection

- Vulnerability of CollegeSource Products: *High, depending on products installed (see chart)*
- General Vulnerability to CollegeSource Clients: *High*
- Recommended Resolution: *Update affected products to latest version.*

The full text of the Spring Security Alert can be found here: *http://support.springsource.com/security/cve-2011-2730* To summarize:

To enable the use of Expression Language (EL) in web applications based on earlier JSP specifications, some Spring MVC tags provide EL support independently of the Servlet/JSP container. The evaluation of EL is enabled by default. When used on containers that do support EL, the attributes can be evaluated for EL twice. Once by the container and once by the tag. This can lead to unexpected results that include disclosure of information and remote code execution (initially only information disclosure was documented but a subsequent report showed the possibility of code execution).

Several CollegeSource products use Spring MVC tags and therefore are vulnerable to Spring Expression Language Injection. The products affected and the recommended resolution are listed in the table below:

CollegeSource Product	Recommended Action
u.direct	update to the latest u.direct release OR update u.direct Spring libraries
Schedule Builder	update to the latest Schedule Builder Release
u.achieve Self-Service	update u.achieve self-service Spring libraries u.achieve self-service release 4.1.2 will include the updated libraries by default (available Feb 28, 2013)
u.select Connector	update to the latest u.select Connector release
u.select	Hosted site has been updated to resolve vulnerability, no client action necessary
u.achieve Server, u.achieve Client	Not affected, no action necessary
DARwin Server, DARwin Client, DARSweb	Not affected, no action necessary
Banner Interface (DARwin and u.achieve)	Not affected, no action necessary
CollegeSource (redLantern) Security	Not affected, no action necessary

TES, CollegeSource Online	Not affected, no action necessary

Java 7 Security Manager Bypass Vulnerability

- Vulnerability of CollegeSource Products: *None*
- General Vulnerability to CollegeSource Clients: *High*
- Recommended Resolution: *Update Java to latest patch, or disable Java in the browser of all desktops*

The full text of the Oracle Security Alert can be found here: http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html To summarize.:

> **Oracle Security Alert for CVE-2013-0422**
>
> **Description**
>
> This Security Alert addresses security issues CVE-2013-0422 (US-CERT Alert TA13-010A - Oracle Java 7 Security Manager Bypass Vulnerability) and another ***vulnerability affecting Java running in web browsers***. ***These vulnerabilities are not applicable to Java running on servers, standalone Java desktop applications or embedded Java applications.*** They also do not affect Oracle server-based software.

CollegeSource does not write Java applets or web start applications, so none of our applications require the use of Java in the browser. We also do not write standalone Java desktop applications or embedded Java applications, only server applications. This security alert does not directly affect CollegeSource products, and running CollegeSource products does not make you more vulnerable to this threat. You could disable Java in the browser of all your desktops and CollegeSource applications would not be adversely affected.

Also, according to details provided at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422 this vulnerability does NOT affect Java 6, only Java 7.