



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

August 12, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2009-048

DATE(S) ISSUED:

8/18/2009

SUBJECT:

Multiple Vulnerabilities Discovered in Adobe Products

OVERVIEW:

Multiple vulnerabilities have been discovered in the Adobe ColdFusion and Adobe JRun applications. Adobe ColdFusion is an application development platform that allows organizations to create dynamically-generated web sites. Adobe JRun is an application server that is used for creating Java-based applications. Some of these vulnerabilities allow an attacker to modify the content of a web site. If a user subsequently visits a specifically crafted web page, or opens a specially crafted file, exploitation may occur. Successful exploitation of these vulnerabilities could allow an attacker to access private information or redirect an unsuspecting user to malicious content.

Proof-of-concept code is publicly available, which may be used to aid in exploiting these vulnerabilities.

SYSTEMS AFFECTED:

- Adobe ColdFusion 7.0.2
- Adobe ColdFusion 8
- Adobe ColdFusion 8.0.1
- Adobe ColdFusion MX 6.1
- Adobe ColdFusion MX 7.00
- Adobe ColdFusion MX 7.01
- Adobe ColdFusion MX 7.02
- Adobe ColdFusion MX Enterprise 6.1
- Adobe ColdFusion MX Enterprise 7.0
- Adobe JRun 4.0 Updater 7 and earlier
- Macromedia JRun 4.0.0
- Macromedia JRun 4.0.0 Service Pack 1a and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been identified in Adobe ColdFusion and Adobe JRun, which include cross-site scripting and unauthorized account access. These vulnerabilities may be exploited if a user visits a specifically crafted web page, or opens a specially crafted file.

Multiple Adobe ColdFusion HTML Injection Vulnerabilities

Adobe ColdFusion is prone to multiple HTML injection vulnerabilities.

Specifically, the following scripts and parameters are affected:

```
'administrator/logviewer/searchlog.cfm': 'startRow'  
'wizards/common/_logintowizard.cfm': URI string  
'wizards/common/_authenticatewizarduser.cfm': URI string  
'administrator/enter.cfm': URI string
```

Successful exploitation would allow for attacker supplied HTML and script code to run in the context of the affected Coldfusion web application, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user.

Adobe JRun Directory Traversal Vulnerability

Adobe JRun is prone to a directory-traversal vulnerability. This issue arises when the application fails to sufficiently sanitize user-supplied input to the 'logfile' parameter of the 'logging/logviewer.jsp' script. This will allow the attacker read-only access to files under the context of the webserver process which could lead to the attacker gaining access to sensitive information such as password files, or system files.

Multiple Adobe ColdFusion and JRun Cross Site Scripting Vulnerabilities

Multiple cross-site scripting vulnerabilities exist in the Adobe ColdFusion and JRun applications. Cross-site scripting vulnerabilities occur due to the failure to sanitize user-supplied input and unfiltered style expressions. Cross-site scripting is an attack that results in execution of script code in the browser of an unsuspecting user. Please note that the cross-site scripting vulnerabilities require user interaction such as clicking on a malicious link.

Adobe ColdFusion Session Fixation Vulnerability

Adobe ColdFusion is prone to a session-fixation vulnerability. Session-fixation is an attack technique that forces a user's session ID to an explicit value. This vulnerability may

be exploited if a user visits a specially crafted webpage. Successful exploitation will allow an attacker to hijack a user's session and gain unauthorized access to the affected Coldfusion web application. For more information about session-fixation please visit the following links:

http://www.webappsec.org/projects/threat/classes/session_fixation.shtml

http://www.acros.si/papers/session_fixation.pdf

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Adobe to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Remind users not to download or open files from un-trusted websites.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Secunia:

<http://www.secunia.com/advisories/36329>

Vupen:

<http://www.vupen.com/english/advisories/2009/2286>

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb09-12.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1872>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1873>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1874>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1875>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1876>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1877>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1878>