

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

05/09/2013

05/14/2013 – UPDATED

SUBJECT:

Adobe ColdFusion Could Allow for Information Disclosure

OVERVIEW:

A vulnerability has been discovered in Adobe ColdFusion which could allow for information disclosure. Adobe ColdFusion is an application server that enables rapid development, deployment, and maintenance of web applications. Multiple versions of the ColdFusion software have been found to be vulnerable and can be exploited with publically available exploit code. Successful exploitation could result in an attacker gaining access to sensitive information.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild.

May 14 – UPDATED OVERVIEW:

Adobe has released a security hotfix for ColdFusion 10, 9.0.2, 9.0.1, and 9.0 for Windows, Macintosh, and UNIX. This hotfix addresses this information disclosure vulnerability.

SYSTEMS AFFECTED:

- Adobe ColdFusion 10
- Adobe ColdFusion 9.0.2
- Adobe ColdFusion 9.0.1
- Adobe ColdFusion 9.0 and earlier versions

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: Low

DESCRIPTION:

Adobe ColdFusion is prone to an information disclosure vulnerability. Using directory traversal techniques an attacker can gain access to directories containing sensitive files and information, including administrator account passwords. Successful exploitation allows remote users to access files stored within the CFIDE/administrator, CFIDE/adminapi, and CFIDE/gettingstarted directories.

There is currently a known working exploit available for this vulnerability. An attacker can leverage this vulnerability on a server that is running ColdFusion software to exploit the issue. If the server is vulnerable, the attack will gain access to admin usernames and passwords.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild.

May 14 – UPDATED DESCRIPTION:

Adobe has released a security hotfix for this information disclosure vulnerability. This fix is available at: <http://helpx.adobe.com/coldfusion/kb/coldfusion-security-hotfix-apsb13-13.html>

RECOMMENDATIONS:

The following actions should be taken:

- Update Adobe ColdFusion on vulnerable systems as soon as fixes become available and proper testing has been completed.
- Restrict public access to the CFIDE/administrator, CFIDE/adminapi, and CFIDE/gettingstarted directories.
- Refer Adobe's to publically available ColdFusion 9 and Coldfusion 10 Lockdown guides.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/advisories/apsa13-03.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3336>

SecurityFocus:

<http://www.securityfocus.com/bid/59773>

May 14 – UPDATED REFERENCES

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb13-13.html>