



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

November 6, 2008

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.

STATE OF ALASKA ADVISORY NUMBER:

2008-024

DATE(S) ISSUED:

11/6/2008

SUBJECT:

Multiple Vulnerabilities Discovered in Adobe Flash Player

OVERVIEW:

Several security vulnerabilities have been identified in Adobe Flash Player. Adobe Flash Player is a widely distributed multimedia and application player for Microsoft Windows, Mozilla, and Apple technologies. It is used to enhance the user experience when visiting web pages or reading email messages. These vulnerabilities can be exploited if a user views a malicious webpage or opens a malicious Shockwave Flash (SWF) or Java Archive (JAR) file. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. If the user is logged in with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Adobe Flash CS4 Professional
- Adobe Flash Player 10
- Adobe Flash Player 7
- Adobe Flash Player 7.0.69.0
- Adobe Flash Player 7.0.70.0
- Adobe Flash Player 8.0.34.0
- Adobe Flash Player 8.0.35.0
- Adobe Flash Player 9
- Adobe Flash Player 9.0.124 .0
- Adobe Flash Player 9.0.28.0
- Adobe Flash Player 9.0.31.0
- Adobe Flash Player 9.0.45.0
- Adobe Flash Player 9.0.47.0
- Adobe Flash Player 9.0.48.0
- Adobe Flash Player 9.0.115.0
- Adobe Flex 3.0

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:

Several new security vulnerabilities have been identified in Adobe Flash Player. These vulnerabilities can be exploited if a user views a malicious webpage or opens a malicious Shockwave Flash (SWF) or Java Archive (JAR) file.

The six reported vulnerabilities include:

- Two Cross-site scripting vulnerabilities which could allow an attacker to direct malicious content to a web browser
- Two Information-disclosure vulnerabilities which may allow an attacker to gather sensitive information
- One DNS Rebinding vulnerability, which could aid an attacker in accessing internal network resources
- One vulnerability which could allow an attacker to bypass security polices

Attackers can exploit these vulnerabilities to steal cookie-based authentication credentials, control how webpages are rendered, or execute arbitrary script code in the context of the application; additional attacks may also be possible.

Adobe has released updates for Adobe Flash Player which address all of the reported vulnerabilities.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to Adobe Flash Player 10.0.12.36 or 9.0.151.0.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from unknown or un-trusted sources.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb08-20.html>

Security Focus:

<http://www.securityfocus.com/bid/32129>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4818>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4819>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4820>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4821>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4822>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4823>