



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

**May 28, 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:**

2008-014

**DATE(S) ISSUED:**

May 28, 2008

**SUBJECT:**

Adobe Flash Player Code Execution Vulnerability

**OVERVIEW:**

Adobe Flash contains a vulnerability that may allow an attacker to run code on a vulnerable system. There are reports that this vulnerability is being actively exploited.

US-CERT has published a Current Activity entry and Vulnerability Note detailing this issue. They are available at:

[http://www.us-cert.gov/current/#adobe\\_flash\\_player\\_vulnerability](http://www.us-cert.gov/current/#adobe_flash_player_vulnerability)

<http://www.kb.cert.org/vuls/id/395473>

**DESCRIPTION:**

The Adobe Flash Player is a player for the Flash media format and enables frame-based animations and multimedia to be viewed within a web browser.

Adobe Flash Player contains an code execution vulnerability. An attacker may be able to trigger this overflow by convincing a user to open a specially crafted SWF file. The SWF file could be hosted or imbedded in a web page. If an attacker can take control of a web site or web server, this vulnerability may be exploited by trusted sites.

**RECOMMENDATIONS:**

We recommend that all of the following actions be considered:

- Upgrade vulnerable systems to Adobe Flash Player 9.0.124.0, after appropriate testing. The upgrade was released on April 8, 2008 and we recommended applying the upgrade in Cyber Advisory 2008-014 dated April 9, 2008.

- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privilege) to diminish the effects of a successful attack.
- If you believe you have been affected by targeted attacks exploiting this vulnerability, please follow your organization's policies for incident reporting.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails, especially from un-trusted sources.

## **REFERENCES:**

### **CVE**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0071>

### **SecurityFocus:**

<http://www.securityfocus.com/bid/29386>

<http://www.securityfocus.com/bid/28695>

### **Symantec:**

[http://www.symantec.com/security\\_response/threatcon/index.jsp](http://www.symantec.com/security_response/threatcon/index.jsp)

### **Mark Dowd:**

[http://documents.iss.net/whitepapers/IBM\\_X-Force\\_WP\\_final.pdf](http://documents.iss.net/whitepapers/IBM_X-Force_WP_final.pdf)

### **ShadowServer:**

<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080527>