



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

April 10, 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:

2008-010

DATE ISSUED:

April 9, 2008

SUBJECT:

A Vulnerability in Adobe Flash Player Allows for Remote Code Execution

OVERVIEW:

Adobe Flash Player is a widely distributed multimedia and application player. It is used to enhance the user experience when visiting web pages or reading email messages. Adobe has released a Flash Player update that addresses multiple vulnerabilities. The most important of these vulnerabilities pertains to the way Flash files are handled and can result in the execution of attacker supplied code. This particular vulnerability can be exploited if a user visits a webpage or opens email with an embedded malicious file. A successful exploit may result in the execution of malicious code with the same system level privileges as the logged in user. This may allow the attacker to take complete control of the affected system.

We are unaware of any publically available exploits for this vulnerability.

SYSTEMS AFFECTED:

- Adobe Flash Player 9.0.115.0 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:

Adobe Flash Player fails to properly handle embedded Actionscript objects with malicious attributes. Specifically, the application fails to properly handle a malformed Shock Wave Flash (SWF) file that contains a 'DeclareFunction2' Actionscript tag. In order to trigger this vulnerability, a user must be enticed to visit a malicious web page or open an email that contains a specially crafted SWF file. Once the file has been executed, the attacker will be able to run arbitrary code in the at the same privilege level as the logged-in user.

We are unaware of any publically available exploits for this vulnerability. Adobe has released Flash Player 9.0.124.0 to address this issue.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable systems to Adobe Flash Player 9.0.124.0, after appropriate testing.
- 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.
- Do not open emails from un-trusted sources.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb08-11.html>

Security Focus:

<http://www.securityfocus.com/bid/28694>

Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-08-021/>

RedHat:

<https://rhn.redhat.com/errata/RHSA-2008-0221.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6019>