



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory
July 18, 2007**

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:

2007-21

DATE ISSUED:

July 18, 2007

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in Adobe Flash Player. This vulnerability can be exploited if a user visits a malicious webpage that hosts a malicious file or opens a malicious email attachment. Successful exploitation may result in the attacker executing malicious code utilizing the same privileges as the victim. For example, if the victim had system administrator privileges, the attacker would have the same privileges. Successful exploitation of this vulnerability could lead to victim's browser to crash, a denial of service or arbitrary code execution.

Adobe Flash Player is installed on many Microsoft Windows, Mac OSX, and Linux/UNIX workstations. Web sites commonly use Adobe Flash for an enhanced viewer experience by providing animations and sound. Therefore, wide spread use of this application coupled with limited user interaction required for exploitation increases the criticality of this vulnerability.

Proof of concept code is available and there are reports of public exploitation.

SYSTEMS AFFECTED:

- RedHat Enterprise Linux Supplementary v.5 server
- RedHat Enterprise Linux Extras v.4
- RedHat Enterprise Linux Extras v.3
- RedHat Enterprise Linux Desktop Supplementary v.5 client
- Macromedia Flash 8.0.24 .0

- Macromedia Flash 8.0.22 .0
- Macromedia Flash 7.0.63 .0
- Macromedia Flash 7.0.61 .0
- Macromedia Flash 7.0.60 .0
- Macromedia Flash 7.0.25 .0
- Macromedia Flash 7.0.19 .0
- Macromedia Flash 7.0 r19
- Macromedia Flash 8.0.33.0
- Macromedia Flash 8.0
- Macromedia Flash 7.0.68.0
- Macromedia Flash 7.0.66.0
- Adobe Flash Player Plugin 9.0.31 .0
- Adobe Flash Player Plugin 9.0.28 .0
- Adobe Flash Player Plugin 9.0.20 .0
- Adobe Flash Player Plugin 9.0.16
- Adobe Flash Player Plugin 8.0
- Adobe Flash Player Plugin 7.0.63
- Adobe Flash Player Plugin 7.0.25
- Adobe Flash Player Plugin 9.0.18d60
- Adobe Flash Player 9.0.45.0
- Adobe Flash Player 9.0.31.0
- Adobe Flash Player 9.0.28.0
- Adobe Flash Player 8.0.34.0
- Adobe Flash Player 7.0.69.0

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:

A new vulnerability has been discovered in Adobe Flash Player pertaining to the way that user-supplied input is handled. More specifically, this is a buffer overflow vulnerability in the way Adobe Flash Player handles the content data types defined in the header portion of the flv video file. Successful exploitation of this vulnerability could lead to client's browser to crash, a denial of service or arbitrary code execution with the same privileges as the user running the application.

Adobe Flash Player is installed on many Microsoft Windows, Mac OSX, and Linux/UNIX workstations since many web applications use it for frame-based animations with sound to be viewed within a web browser. Therefore, wide spread use of this application coupled with limited user interaction required for exploitation increases the criticality of this vulnerability.

Proof of concept code is available and there are reports of public exploitation.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply all the appropriate patches provided by Adobe to vulnerable systems immediately after appropriate testing.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from un-trusted sources.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb07-12.html>

Security Focus:

<http://www.securityfocus.com/bid/24856>

Minded Security:

http://www.mindedsecurity.com/en/labs/advisories/flash_remote_flv_exec

US-CERT:

<http://www.kb.cert.org/vuls/id/730785>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3456>