

Enterprise Technology Services



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

February 25, 2009

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:

SA2009-014

DATE(S) ISSUED:

02/25/09

Subject:

Multiple Vulnerabilities Discovered in Adobe Flash Player

Source:

MS-ISAC

Systems Affected:

- Adobe Flash CS4 Professional
- Adobe Flash Player 10.0.12.36 and earlier (Adobe Flash Player 10.0.15.3 and earlier for Linux)
- 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

Overview:

Four new security vulnerabilities have been identified in Adobe Flash Player. These vulnerabilities can be exploited if a user visits a malicious website or opens an email containing a Flash media file designed to trigger these issues.

Details of these vulnerabilities are:

- A remote code-execution vulnerability which occurs when a user loads a malicious Shockwave Flash file (.SWF) that fails to properly de-allocate memory when an object is

destroyed. The reference to the improperly de-allocated memory can then be used by the attacker to gain arbitrary execution control by re-allocating the memory used by the destroyed object.

- Two “Clickjacking” Security Bypass vulnerabilities that can be exploited to bypass security restrictions and disclose information. Clickjacking is a malicious technique that involves embedding code or a script into a web page that tricks a user into performing unintended actions. This occurs when a user mistakenly clicks on a concealed link or when the user clicks on a button that triggers the malicious action.
- A remote Denial of Service (DoS) vulnerability occurs because Adobe Flash Player fails to validate user-supplied input.

Attackers can exploit these vulnerabilities to disclose information, control how web pages are rendered, cause DoS conditions, or execute arbitrary script code in the context of the logged on user. Additional attacks may also be possible. Successful exploitation of the first two vulnerabilities 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. Failed attempts may result in DoS conditions.

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

Recommendations / Resolution:

We recommend the following actions be taken:

- Upgrade to the recommended software version based on Adobe's security advisory
- 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/apsb09-01.html>
- <http://www.adobe.com/products/flash/>

Security Focus:

- <http://www.securityfocus.com/bid/33889>
- <http://www.securityfocus.com/bid/33890>
- <http://www.securityfocus.com/bid/33880>
- <http://www.securityfocus.com/archive/1/49A43D67.3080609@idefense.com>

CVE:

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0519>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0520>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0521>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0522>

Secunia:

- <http://secunia.com/advisories/34012>