



State of Alaska
State Security Office

Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory
July 29, 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:

SA2009-039

DATE(S) ISSUED:

07/29/09

Subject:

Adobe Flash/Shockwave, ISC-BIND, Microsoft vulnerabilities

Source:

MS-ISAC / Adobe / Microsoft

Adobe:

Systems Affected:

- Flash / Shockwave players

Overview:

Adobe has released Shockware Player 11.5.1.601 because previous versions used a vulnerable version of the Microsoft Active Template Library (ATL). Additionally, Adobe has released a security advisory to address the same issue in Flash Player. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.

The security advisory for Flash Player indicates that Adobe will be releasing fixes for this issue on July 30, 2009. In the interim, the advisory suggests that users consider installing the Cumulative Security Update for Internet Explorer as defined in Microsoft Security Bulletin MS09-034 to help mitigate some of the risks until fixes are available.

Recommendations / Resolution:

SSO encourages users and administrators to review Adobe documents APSP09-11 and APSA09-04 and apply any necessary updates to help mitigate the risks. Additional information can be found in the Adobe PSIRT blog.

References:

<http://www.microsoft.com/technet/security/bulletin/ms09-034.msp>

http://blogs.adobe.com/psirt/2009/07/impact_of_microsoft_atl_vulner.html

<http://www.adobe.com/support/security/advisories/apsa09-04.html>

<http://www.adobe.com/support/security/bulletins/apsb09-11.html>

Microsoft**Systems Affected:**

- Microsoft Windows and Windows Server
- Microsoft Internet Explorer
- Microsoft Visual Studio and C++ Redistributable Package
- ActiveX controls from multiple vendors

Overview:

Microsoft has released two out-of-band security bulletins. The first bulletin, MS09-034, is a cumulative security update for Internet Explorer that addresses several vulnerabilities. These vulnerabilities may allow a remote attacker to execute arbitrary code. The second bulletin, MS09-035, addresses vulnerabilities in the Visual Studio Active Template Library (ATL). Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.

Additionally, Microsoft has released security advisory 973882 to provide specific guidance for developers, IT professionals, consumers, and home users regarding the vulnerabilities in Active Template Library (ATL).

Recommendations / Resolution:

SSO encourages users and administrators to review Microsoft Security Bulletins MS09-034 and MS09-035 and Microsoft Security Advisory 973882 and apply any necessary updates or workarounds to help mitigate the risks. Additional information can be found in Technical Cyber Security Alert TA09-209A.

References:

<http://www.microsoft.com/technet/security/bulletin/ms09-034.msp>

<http://www.microsoft.com/technet/security/bulletin/ms09-035.msp>

<http://www.us-cert.gov/cas/techalerts/TA09-209A.html>

<http://www.microsoft.com/technet/security/advisory/973882.msp>

ISC-BIND**Overview:**

The Internet Systems Consortium (ISC) has released BIND versions 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 to address a vulnerability. By sending a specially crafted dynamic update packet to an affected BIND 9 server, a remote, unauthenticated attacker may be able to cause a denial-of-service condition.

Recommendations / Resolution:

US-CERT encourages users and administrators to review the Internet Systems Consortium advisory and apply any necessary updates to help mitigate the risks. Additional information can be found in the Vulnerability Notes Database.

References:

<https://www.isc.org/node/474>

<http://www.kb.cert.org/vuls/id/725188>