

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 11, 2010

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.

ADVISORY NUMBER:

SA2010-061

DATE(S) ISSUED:

8/11/2010

SUBJECT:

Multiple Adobe Flash Media Server Remote Security Vulnerabilities

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Flash Media Server that could allow an attacker to take complete control of an application. Adobe Flash Media Server is an application server product which can stream rich content applications. Successful exploitation of one of these vulnerabilities could result in remote code execution. The attacker could then perform actions in the context of the application. The remaining vulnerabilities could allow for a denial-of-service condition.

SYSTEMS AFFECTED:

- Adobe Flash Media Server (FMS) 3.5.3 and earlier for Windows and UNIX
- Adobe Flash Media Server 3.0.5 and earlier versions for Windows and UNIX

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

DESCRIPTION:

Four vulnerabilities have been discovered in Adobe Flash Media Server. These vulnerabilities are as follows:

- A remote arbitrary code execution vulnerability caused by a Javascript method issue.
- A denial of service vulnerability caused by a Javascript method vulnerability.
- A denial of service vulnerability caused by ScriptLib netservices.asc which has an unshift function that, when included in applications, exposes a potential memory exhaustion attack on server applications.
- A denial of service vulnerability caused by an input validation issue.

Successful exploitation of one of these vulnerabilities could result in remote code execution. The attacker could then perform actions in the context of the application. The remaining vulnerabilities could allow for a denial-of-service condition.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the appropriate updates which have been provided by Adobe to vulnerable systems immediately after appropriate testing.
- Systems running Adobe Flash Media Server 3.5.3 and earlier versions should be updated to version 3.5.4.
- Systems running Adobe Flash Media Server 3.0.5 and earlier versions should be updated to version 3.0.6.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb10-19.html>

Security Focus:

<http://www.securityfocus.com/bid/42352>

<http://www.securityfocus.com/bid/42354>

<http://www.securityfocus.com/bid/42356>

<http://www.securityfocus.com/bid/42357>

Secunia:

<http://secunia.com/advisories/40910/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2217>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2218>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2219>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2220>