



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

**November 8, 2012**

*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:**

SA2012-070

**DATE(S) ISSUED:**

11/08/2012

**SUBJECT:**

Unspecified Remote Code Execution Vulnerability in Adobe Reader

**OVERVIEW:**

An unspecified Remote Code Execution (RCE) vulnerability has been discovered in Adobe Reader that could allow an attacker to take control of the affected system. Adobe Reader allows users to view Portable Document Format (PDF) files. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**SYSTEMS AFFECTED:**

- Adobe Reader X (version 10 and earlier)
- Adobe Reader XI (version 11)

**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 Reader is prone to an unspecified remote code execution vulnerability that could allow for remote code execution. Members of the computer security community have observed an exploit targeting Adobe Reader X and Adobe Reader XI being used by the Blackhole exploit kit, which is used to distribute various strains of malware including Zeus, Spyeye, Carberp, and Citadel.

Adobe has stated that they have not verified this vulnerability, and are in the process of investigating the claim. According to researchers at Group-IB, this vulnerability allows for bypassing of the sandbox feature in Adobe Reader. Group-IB also states that the exploit does not fully work until a user closes Adobe Reader or a web browser using the Adobe Reader plugin.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply the update provided by Adobe, after appropriate testing, as soon as it becomes available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

#### **REFERENCES:**

##### **Group-IB:**

<http://www.group-ib.com/index.php/7-novosti/672-group-ib-us-zero-day-vulnerability-found-in-adobe-x>

##### **Krebs on Security:**

<http://krebsonsecurity.com/2012/11/experts-warn-of-zero-day-exploit-for-adobe-reader/>