



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

**July 14, 2015**

*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:  
SA2015-078**

**DATE(S) ISSUED:  
07/14/2015**

**SUBJECT:  
Multiple Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution (APSB15-15)**

**OVERVIEW:**  
Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat. Adobe Reader and Acrobat are applications for handling PDF files. Attackers can exploit these issues to execute arbitrary code within the context of the affected application. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or compromising processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

**THREAT INTELLIGENCE**  
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Adobe Reader XI (11.0.11) and earlier 11.x versions
- Adobe Reader X (10.1.14) and earlier 10.x versions
- Adobe Acrobat XI (11.0.11) and earlier 11.x versions
- Adobe Acrobat X (10.1.13) and earlier 10.x versions
- Adobe Acrobat DC (2015.007.20033) Continuous
- Adobe Reader DC (2015.007.20033) Continuous
- Adobe Acrobat DC (2015.006.30033) Classic
- Adobe Reader DC (2015.006.30033) Classic

**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

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Adobe Reader and Adobe Acrobat that could potentially allow an attacker to take over the affected system.

- Buffer overflow vulnerability that could lead to code execution (CVE-2015-5093).
- Heap buffer overflow vulnerabilities that could lead to code execution (CVE-2015-5096, CVE-2015-5098, CVE-2015-5105).
- Memory corruption vulnerabilities that could lead to code execution (CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, CVE-2015-3095, CVE-2015-5115, CVE-2014-0566).
- An information leak vulnerability (CVE-2015-5107).
- Security bypass vulnerabilities that could lead to information disclosure (CVE-2015-4449, CVE-2015-4450, CVE-2015-5088, CVE-2015-5089, CVE-2015-5092, CVE-2014-8450).
- Stack overflow vulnerability that could lead to code execution (CVE-2015-5110).
- Use-after-free vulnerabilities that could lead to code execution (CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, CVE-2015-5114).
- Validation bypass issues that could be exploited to perform privilege escalation from low to medium integrity level (CVE-2015-4446, CVE-2015-5090, CVE-2015-5106).
- Validation bypass issue that could be exploited to cause a denial-of-service condition on the affected system (CVE-2015-5091).
- Integer overflow vulnerabilities that could lead to code execution (CVE-2015-5097, CVE-2015-5108, CVE-2015-5109).
- Various methods to bypass restrictions on JavaScript API execution (CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, CVE-2015-5086).
- Null-pointer dereference issues that could lead to a denial-of-service condition (CVE-2015-4443, CVE-2015-4444).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or compromising processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

**REFERENCES:****Adobe:**

<https://helpx.adobe.com/security/products/reader/apsb15-15.html>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0566>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8450>

