

# EOC Information Alert

**02/08/2011**

**DATE(S) ISSUED:**

2/8/2011

**SUBJECT:**

Multiple Vulnerabilities Discovered in Adobe Products

**OVERVIEW:**

Twenty-nine vulnerabilities have been discovered in the Adobe Reader and Adobe Acrobat applications, which could allow an attacker to take complete control of an affected system. Adobe Reader allows users to view Portable Document Format (PDF) files while Adobe Acrobat offers users additional features such as the ability to create PDF files. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted PDF file. Successful exploitation will 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 (10.0) and earlier for Windows and Macintosh.
- Adobe Reader 9.4.1 and earlier for Windows, Macintosh and UNIX.
- Adobe Acrobat X (10.0) and earlier for Windows and Macintosh.

**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:** Twenty-nine security vulnerabilities have been identified in Adobe Reader and Adobe Acrobat. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing a file designed to trigger these issues. The vulnerabilities are as follows:

- Two input validation vulnerabilities that could lead to code execution (CVE-2010-4091) (CVE-2011-0586).
- Two input validation vulnerabilities that could lead to a cross-site scripting vulnerability (CVE-2011-0587) (CVE-2011-0604).
- Three library-loading vulnerability that could lead to code execution (CVE-2011-0562) (CVE-2011-0570) (CVE-2011-0588)
- Four memory corruption vulnerability that could lead to code execution (CVE-2011-0563) (CVE-2011-0606) (CVE-2011-0589) (CVE-2011-0605 - Macintosh only).
- One Windows-only file permissions issue that could lead to privilege escalation (CVE-2011-0564).
- Three denial of service vulnerabilities; arbitrary code execution has not been demonstrated, but may be possible (CVE-2011-0565), (CVE-2011-0585) (CVE-2011-0568 - Macintosh only).
- Seven image-parsing memory corruption vulnerabilities that could lead to code execution (CVE-2011-0596)(CVE-2011-0598)(CVE-2011-0599)(CVE-2011-0602)(CVE-2011-0566)(CVE-2011-0567)(CVE-2011-0603).
- Six 3D file parsing input validation vulnerabilities that could lead to code execution (CVE-2011-0590)(CVE-2011-0591)(CVE-2011-0592)(CVE-2011-0593)(CVE-2011-0595)(CVE-2011-0600).
- One font parsing input validation vulnerability that could lead to code execution (CVE-2011-0594).

Successful exploitation may result in an attacker gaining the same user 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.

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

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

#### **REFERENCES:**

##### **Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb11-03.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4091>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0562>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0563>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0564>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0565>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0566>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0567>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0568>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0570>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0585>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0586>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0587>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0588>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0589>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0590>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0591>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0592>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0593>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0594>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0595>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0596>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0598>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0599>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0600>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0602>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0603>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0604>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0605>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0606>

EOC  
490 18<sup>th</sup> Street  
Helena, MT 59601  
24x7 Operations Line (406) 444-2000  
1-800-628-4917