COT Security Alert – Adobe Remote Code Execution Vulnerabilities

---

Adobe reports vulnerabilities in certain versions of Adobe Reader and Acrobat which could allow an attacker to gain control of an affected system. An attacker could gain access to install programs; view, change or delete data; or create new accounts with full user rights, depending on the privileges associated with the logged-on user. A denial-of-service (DoS) condition could occur in the case of failed exploit attempts. Sources have reported to Adobe that some of these vulnerabilities are being actively exploited in limited, targeted attacks, mainly against Adobe Reader 9.x on Microsoft Windows.

This exploit has a high risk factor for business, government and home users. The vulnerabilities include four memory corruption vulnerabilities, one heap corruption vulnerability and one U3D memory corruption vulnerability.

Versions affected:

Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh
Adobe Reader 9.4.7 and earlier 9.x versions for Windows, Macintosh and UNIX
Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
Adobe Acrobat 9.4.7 and earlier 9.x versions for Windows and Macintosh

Take the following actions to reduce or mitigate risk:

- Users of Adobe Acrobat or Reader 9.4.7 and earlier 9.x versions for Windows and Macintosh update to version 9.5.
- Users of Adobe Acrobat and Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh update to version 10.1.2.
- Consider running Adobe Reader X in Protected Mode.
- 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.

Information about these vulnerabilities may be found at:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb12-01.html
http://www.adobe.com/support/security/advisories/apsa11-04.html
http://www.adobe.com/support/security/bulletins/apsb11-30.html

CVE:
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4369
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4370
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4371
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4372
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4373

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/CISO/