



Security Alert: Vulnerabilities Involving Adobe Acrobat Reader and JavaScript

Adobe Systems Incorporated and various news outlets have announced the existence of two new vulnerabilities in the Adobe Acrobat Reader application.

Details

The vulnerabilities (Bugtraq IDs 34736 and 34740) stem from the JavaScript functions *getAnnots* and *spell.customDictionaryOpen*. While Trustwave is not aware of reports of widespread exploitation of the vulnerabilities, demonstration exploits have been publicized (see <http://www.milw0rm.com/exploits/8570> and <http://www.milw0rm.com/exploits/8569>). All Reader versions currently supported by Adobe are vulnerable to the exploits. These vulnerabilities could allow an attacker to compromise a machine running the software and either crash the application or take control of the system.

Protecting Your Organization

Adobe has publicized these vulnerabilities and expects to release patches by May 12, 2009. In the meantime, there are steps you can take to protect your systems:

- Perhaps most importantly, do not open unsolicited PDF files from untrusted sources.
- Secondly, Adobe recommends disabling JavaScript within Adobe Reader to prevent attackers from exploiting these vulnerabilities.
- For more precautionary measures you can take to further protect yourself, please see <http://www.kb.cert.org/vuls/id/970180>.

Sources

“Adobe Product Security Incident Response Team (PSIT): Adobe Reader Issue Update” Adobe Blogs. http://blogs.adobe.com/psirt/2009/05/adobe_reader_issue_update.html (accessed May 4, 2009).

“Adobe Reader ‘getAnnots()’ JavaScript Function Remote Code Execution Vulnerability.” SecurityFocus. <http://www.securityfocus.com/bid/34736/> (accessed May 4, 2009).

“Adobe Reader ‘spell.customDictionaryOpen()’ JavaScript Function Remote Code Execution Vulnerability.” SecurityFocus. <http://www.securityfocus.com/bid/34740/> (accessed May 4, 2009).

“Adobe confirms new flaw, recommends turning off JavaScript - SC Magazine US.” Security News and Security Product Reviews - SC Magazine US. http://www.scmagazineus.com/Adobe-confirms-new-flaw-recommends-turning-off-JavaScript/article/131576/?DCMP=EMC-SCUS_Newsire (accessed May 4, 2009).

“US-CERT Vulnerability Note VU#970180.” CERT Knowledge-base. <http://www.kb.cert.org/vuls/id/970180> (accessed May 4, 2009).