security-assessment.com

Vulnerability Advisory

Name	Malformed .joboptions File Effecting Adobe Acrobat Distiller v8
Vendor Website	http://www.adobe.com
Date Released	14 May, 2008
Affected Software	Adobe Acrobat Professional v8
Researcher	Paul Craig : paul.craig@security-assessment.com

Description

Original Adobe Advisory: APSA08-01
(http://www.adobe.com/support/security/advisories/apsa08-01.html)

Security-Assessment.com has discovered multiple heap based overflow flaws within Acrobat Distiller 8 which under certain circumstances be used to execute arbitrary code.
The PDF quality settings file, .joboptions used by Distiller was found to contain two heap based overflows.

Font names stored within the parameters /AlwaysEmbed and /NeverEmbed both produce a similar heap based overflow when a large (160+ char) font name is supplied.

Acrobat 8 professional and any other Adobe suite which contains Acrobat 8 acrodist.exe (Such as CS3) is vulnerable to this issue.

Security-Assessment.com was able to gain code execution on a Windows XP SP2 machine through this Issue. However, reliability of the exploit was low as it relies on a specific heap structure being present. Only a 20% success rate was possible.

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team members have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093