Vulnerability Advisory

Name	Multiple Flash Authoring Heap Overflows - Malformed SWF Files
Vendor Website	http://www.adobe.com
Date Released	October 16, 2008
Affected Software	Flash CS3 Professional Windows Platform / Flash MX 2004
Researcher	Paul Craig - paul.craig@security-assessment.com
References	CVE: CVE-2008-4473 : APSA08-09

Description

During analysis of the SWF file format used by commercial Flash authoring applications multiple heap overflows were discovered within Adobe Flash CS3 Professional and Adobe Flash MX 2004.

Heap overflow conditions occurred when opening or importing malformed .SWF files within the Flash authoring applications.
Exploitable conditions were related to excessively long control parameters within an SWF file, which resulted in a heap overflow condition.
Exploitation of the heap overflow conditions would allow a malicious user to gain command execution on the system which opened the file.

Only the Flash authoring software was found to insecurely parse malformed .SWF files.
The Flash player was NOT found to be vulnerable to these specific attacks.

Solution

A patch has been released from Adobe to address this vulnerability within CS3.
Additionally Adobe Flash CS4 has been officially released which resolves these particular vulnerabilities.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

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