**<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1516>**

**Vulnerability Summary for CVE-2010-1516**

**Original release date:**08/17/2010

**Last revised:**08/18/2010

**Source:** US-CERT/NIST

**Overview**

Multiple integer overflows in SWFTools 0.9.1 allow remote attackers to execute arbitrary code via (1) a crafted PNG file, related to the getPNG function in lib/png.c; or (2) a crafted JPEG file, related to the jpeg\_load function in lib/jpeg.c.

**http://secunia.com/secunia\_research/2010-80/**

|  |  |
| --- | --- |
| Secunia Research: SWFTools Two Integer Overflow Vulnerabilities | |
| ======================================================================  Secunia Research 13/08/2010  - SWFTools Two Integer Overflow Vulnerabilities -  ======================================================================  Table of Contents  Affected Software....................................................1  Severity.............................................................2  Vendor's Description of Software.....................................3  Description of Vulnerability.........................................4  Solution.............................................................5  Time Table...........................................................6  Credits..............................................................7  References...........................................................8  About Secunia........................................................9  Verification........................................................10  ======================================================================  1) Affected Software  \* SWFTools 0.9.1  NOTE: Other versions may also be affected.  ======================================================================  2) Severity  Rating: Moderately critical  Impact: System access  Where: Remote  ======================================================================  3) Vendor's Description of Software  "SWFTools is a collection of utilities for working with Adobe Flash  files (SWF files)."  Product Link:  http://www.swftools.org/  ======================================================================  4) Description of Vulnerability  Secunia Research has discovered two vulnerabilities in SWFTools, which  can be exploited by malicious people to compromise a user's system.  1) An integer overflow error within the "getPNG()" function in  lib/png.c can be exploited to cause a heap-based buffer overflow via  specially crafted PNG images.  2) An integer overflow error within the "jpeg\_load()" function in  lib/jpeg.c can be exploited to cause a heap-based buffer overflow via  specially crafted JPEG images.  ======================================================================  5) Solution  Fixed in the GIT repository.  ======================================================================  6) Time Table  10/06/2010 - Vendor notified.  10/06/2010 - Vendor response.  13/08/2010 - Public disclosure.  ======================================================================  7) Credits  Discovered by Stefan Cornelius, Secunia Research.  ======================================================================  8) References  The Common Vulnerabilities and Exposures (CVE) project has assigned  CVE-2010-1516 for the vulnerabilities.  ======================================================================  9) About Secunia  Secunia offers vulnerability management solutions to corporate  customers with verified and reliable vulnerability intelligence  relevant to their specific system configuration:  http://secunia.com/advisories/business\_solutions/  Secunia also provides a publicly accessible and comprehensive advisory  database as a service to the security community and private  individuals, who are interested in or concerned about IT-security.  http://secunia.com/advisories/  Secunia believes that it is important to support the community and to  do active vulnerability research in order to aid improving the  security and reliability of software in general:  http://secunia.com/secunia\_research/  Secunia regularly hires new skilled team members. Check the URL below  to see currently vacant positions:  http://secunia.com/corporate/jobs/  Secunia offers a FREE mailing list called Secunia Security Advisories:  http://secunia.com/advisories/mailing\_lists/  ======================================================================  10) Verification  Please verify this advisory by visiting the Secunia website:  http://secunia.com/secunia\_research/2010-80/  Complete list of vulnerability reports published by Secunia Research:  http://secunia.com/secunia\_research/  ====================================================================== |  |