**<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4988>**

**Vulnerability Summary for CVE-2007-4988**

**Original release date:**09/24/2007

**Last revised:**08/21/2010

**Source:** US-CERT/NIST

**Overview**

Sign extension error in the ReadDIBImage function in ImageMagick before 6.3.5-9 allows context-dependent attackers to execute arbitrary code via a crafted width value in an image file, which triggers an integer overflow and a heap-based buffer overflow.

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=597>

Multiple Vendor ImageMagick Sign Extension Vulnerability

I. BACKGROUND

ImageMagick is a suite of image manipulation tools (animate, composite, conjure, convert, display, identify, import, mogrify and montage) that are sometimes used by other applications for processing image files. For more information about ImageMagick, visit the vendor's site at the following URL.

http://www.imagemagick.org/

II. DESCRIPTION

Remote exploitation of a sign extension vulnerability in ImageMagick, as included in various vendors' operating system distributions, allows attackers to execute arbitrary code.

This vulnerability specifically exists in the ReadDIBImage() as shown below.

558 image->columns=(unsigned long) dib\_info.width

...

620 bytes\_per\_line=4\*((image->columns\*dib\_info.bits\_per\_pixel+31)/32);

621 length=bytes\_per\_line\*image->rows;

622 pixels=(unsigned char \*) AcquireMagickMemory((size\_t) MagickMax(

623 bytes\_per\_line,image->columns+256)\*image->rows\*sizeof(\*pixels));

...

629 count=ReadBlob(image,length,pixels);

...

638 status=DecodeImage(image,dib\_info.compression ? MagickTrue : MagickFalse,pixels);

At line 558, "dib\_info.width" is a signed short, which is extended to an unsigned long and assigned to "image->columns". For example, a value of 0x8000 will be extended to 0xffff8000. Later, it is used as a multiplier when calculating the allocation size. An integer overflow occurs, leading to a heap block of insufficient size being allocated. Consequently, a heap buffer overflow occurs.

III. ANALYSIS

Exploitation of this vulnerability allows an attacker to execute arbitrary code in the context of the user.

One way of exploiting this vulnerability is to persuade a targeted user to open a malicious image file with a program that utilizes the ImageMagick library.

As the tools that are part of ImageMagick are sometimes used as helper tools by other applications, this user may be the same as the web server user. This scenario is somewhat more severe than the previously described attack vector since the image processing can occur automatically.

IV. DETECTION

iDefense Labs confirmed that ImageMagick version 6.3.4 is vulnerable. It is suspected that other versions of ImageMagick are also vulnerable.

V. WORKAROUND

Exposure to this vulnerability can be mitigated by moving or deleting the related module files. The file locations may vary between distributions. The globbing expression listed below corresponds to a Red Hat Linux system.

/usr/lib/ImageMagick-\*/modules\*/coders/dib.\*

VI. VENDOR RESPONSE

The ImageMagick maintainers have addressed this vulnerability with the release of version 6.3.5-9. More information is available from the following URL.

http://studio.imagemagick.org/pipermail/magick-announce/2007-September

/000037.html

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2007-4988 to this issue. This is a candidate for inclusion in the CVE list (http://cve.mitre.org/), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

09/04/2007 Initial vendor notification

09/05/2007 Initial vendor response

09/19/2007 Public disclosure

IX. CREDIT

This vulnerability was reported to iDefense by regenrecht.

Get paid for vulnerability research

http://labs.idefense.com/methodology/vulnerability/vcp.php

Free tools, research and upcoming events

http://labs.idefense.com/

X. LEGAL NOTICES

Copyright � 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customer service for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.