

[VulnWatch] iDEFENSE Security Advisory 07.05.05: Adobe Acrobat Reader UnixAppOpenFilePerform() Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-07/0004.html>

From: iDEFENSE Labs (labs-no-reply_at_idefense.com)

Date: 07/05/05

Date: Tue, 5 Jul 2005 16:25:08 -0400

To: <bugtraq@securityfocus.com>, <vulnwatch@vulnwatch.org>, <full-disclosure@lists.grok.org.uk>

Adobe Acrobat Reader UnixAppOpenFilePerform() Buffer Overflow
Vulnerability

iDEFENSE Security Advisory 07.05.05

www.idefense.com/application/poi/display?id=279&type=vulnerabilities

July 05, 2005

I. BACKGROUND

Adobe Acrobat Reader is a program for viewing Portable Document Format (PDF) documents. More information is available at the following site:

<http://www.adobe.com/products/acrobat/readermain.html>

II. DESCRIPTION

Remote exploitation of a buffer overflow in Adobe Acrobat Reader for Unix could allow an attacker to execute arbitrary code.

The vulnerability specifically exists in the function `UnixAppOpenFilePerform()`. This routine is called by Acrobat Reader while

opening a document containing a `/Filespec` tag. Within this routine, `sprintf` is used to copy user-supplied data into a fixed-sized stack buffer. This leads to a stack based overflow and the execution of arbitrary code. The following demonstrates what the overflow looks like in a debugger:

```
#0 0x41414141 in ?? ()
```

```
(gdb) i r ebx
```

```
ebx 0xbffff54 -1073746092
```

```
(gdb) x/x 0xbffff54
```

0xbffff54: 0x40404040
(gdb)

As shown, EIP is easily controllable; ebx also points to the 4 bytes before the EIP overwrite in a controlled buffer. This allows remote exploitation without having to know stack addresses, as an attacker can craft an exploit to return to a jmp ebx or call ebx instruction.

III. ANALYSIS

Successful exploitation allows an attacker to execute arbitrary code under the privileges of the local user. Remote exploitation is possible via e-mail attachment or link to the maliciously crafted PDF document. The impact of this vulnerability is lessened by the fact that two error messages appear before exploitation is successful; however, closing these windows does not prevent exploitation from occurring.

IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in Adobe Acrobat Reader version 5.0.9 for Unix and Adobe Acrobat Reader version 5.0.10 for Unix. Adobe Acrobat for Windows is not affected. Adobe Acrobat 7.0 for Unix is not affected.

V. WORKAROUND

User awareness is the best defense against this class of attack. Users should be aware of the existence of such attacks and proceed with caution when following links from suspicious or unsolicited e-mail. Users should consider using an unaffected version of Adobe Acrobat, such as Acrobat 7.0

VI. VENDOR RESPONSE

Adobe has addressed this issue in the following security advisory:

<http://www.adobe.com/support/techdocs/329083.html>

Adobe is recommending the following steps for remediation:

— If you use Adobe Reader 5.0.9 or 5.0.10 on Linux or Solaris, download Adobe Reader 7.0 at www.adobe.com/products/acrobat/readstep2.html.

— If you use Adobe Reader 5.0.9 or 5.0.10 on IBM-AIX or HP-UX, download Adobe Reader 5.0.11 at www.adobe.com/products/acrobat/readstep2.html.

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2005-1625 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

05/12/2005 Initial vendor notification
05/12/2005 Initial vendor response
07/05/2005 Public disclosure

IX. CREDIT

iDEFENSE Labs is credited with this discovery.

Get paid for vulnerability research
<http://www.idefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events
<http://labs.idefense.com>

X. LEGAL NOTICES

Copyright (c) 2005 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 email customerservice@idefense.com 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.