

[VulnWatch] iDEFENSE Security Advisory 01.14.05: Exim dns_buld_reverse() Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-01/0029.html>

From: customer service mailbox (customerservice_at_idefense.com)

Date: 01/14/05

Date: Fri, 14 Jan 2005 12:45:28 -0500

To: <bugtraq@securityfocus.com>, <vulnwatch@vulnwatch.org>

Exim dns_buld_reverse() Buffer Overflow Vulnerability

iDEFENSE Security Advisory 01.14.05

www.idefense.com/application/poi/display?id=183&type=vulnerabilities

January 14, 2005

I. BACKGROUND

Exim is a mail transfer agent (MTA) for Unix systems similar to sendmail. More information is available at the following URL:

<http://www.exim.org/>

II. DESCRIPTION

Local exploitation of a buffer overflow vulnerability in Exim 4.41 may allow execution of arbitrary commands with elevated privileges.

The problem specifically exists in the dns_build_reverse() function. The

function fails to check the length of a string which it copies into a fixed length buffer. This string is user controlled and passed into the program from a command line option.

The following example demonstrates an input that will crash Exim:

```
/usr/bin/exim -bh ::%A`perl -e 'print pack('L',0xdeadbeef) x 256`
```

III. ANALYSIS

Exploitation of this vulnerability will give an attacker access to the mailer uid. (The exim mailer is setuid root, but drops privileges before

the vulnerable code is reached). Having the mailer uid may allow access to sensitive information in email messages, or possibly further elevation.

IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in Exim versions 4.40 and 4.41. A source audit of version 4.42 suggests that it is also vulnerable. It is suspected that earlier versions are also vulnerable.

V. WORKAROUND

iDEFENSE is currently unaware of any effective workarounds for this vulnerability.

VI. VENDOR RESPONSE

A patch for Exim release 4.43 which addresses this vulnerability is available at:

<http://www.exim.org/mail-archives/exim-announce/2005/msg00000.html>

The patch will be incorporated into a future Exim release (4.50).

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

09/30/2004 Initial vendor notification
09/30/2004 Initial vendor response
01/14/2005 Public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

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

X. LEGAL NOTICES

Copyright (c) 2004 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.