

[VulnWatch] iDefense Security Advisory 03.28.07: IBM Lotus Domino Server LDAP Request Invalid DN Message Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-03/msg00022.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Wed, 28 Mar 2007 11:30:48 -0400
-

IBM Lotus Domino Server LDAP Request Invalid DN Message Heap Overflow
Vulnerability

iDefense Security Advisory 03.28.07
<http://labs.iddefense.com/intelligence/vulnerabilities/>
Mar 28, 2007

I. BACKGROUND

IBM Lotus Domino Server software provides messaging, calendaring and scheduling capabilities on a variety of operating systems. More information about the product is available at the following URL.

<http://www-142.ibm.com/software/sw-lotus/domino>

II. DESCRIPTION

Remote exploitation of a heap overflow vulnerability in the LDAP component of IBM Corp.'s Lotus Domino Server 7.0.1 may allow a remote attacker to cause denial of service or execute arbitrary code.

When a malformed request is made to the LDAP component of a Lotus Domino Enterprise Server, a heap overflow can be triggered. The vulnerability specifically exists in the handling of strings larger than 65535 bytes. When a string longer than this value is encountered, the service allocates memory using only the lower 16-bits of the string length. Since the entire string is subsequently copied into the newly allocated buffer, a heap-overflow occurs.

III. ANALYSIS

Exploitation of this vulnerability allows attackers to crash the LDAP service or potentially execute arbitrary code on the affected host.

In order to attempt exploitation, attackers must be able to connect to the LDAP service.

Although the service does not run as root, it does run as the same user as many other components of the Lotus Domino Server. Because of this an attacker may gain access to sensitive information or be able to maliciously subvert the server in other ways.

IV. DETECTION

This vulnerability has been confirmed to exist within versions 7.0.1 and 7.0.1.1 the Directory Service (LDAP) component of Lotus Domino Server.

V. WORKAROUND

iDefense is currently unaware of any effective workaround for this issue.

VI. VENDOR RESPONSE

IBM Lotus has addressed this vulnerability in the 6.5.6 and 7.0.2 FP1 releases of Domino. For more information consult IBM Technote swg21257248 via the following URL.

<http://www-1.ibm.com/support/docview.wss?uid=swg21257248>

VII. CVE INFORMATION

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

VIII. DISCLOSURE TIMELINE

10/09/2006 Initial vendor notification
10/10/2006 Initial vendor response
03/28/2007 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

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 customerservice@xxxxxxxxxxxxx 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.