

iDefense Security Advisory 03.23.07: Sun Java System Directory Server 5.2 Uninitialized Pointer Cleanup Design Error Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-03/msg00382.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Fri, 23 Mar 2007 14:11:38 -0400
-

Sun Java System Directory Server 5.2 Uninitialized Pointer Cleanup Design Error Vulnerability

iDefense Security Advisory 03.23.07
<http://labs.idefense.com/intelligence/vulnerabilities/>
Mar 23, 2007

I. BACKGROUND

Sun Java System Directory Server is an LDAP server distributed by Sun with multiple products. More information is available at the following URL.

http://www.sun.com/software/products/directory_srvr/home_directory.xml

II. DESCRIPTION

Remote exploitation of a design error vulnerability in Sun Microsystems Inc.'s Java System Directory Server 5.2 may cause a denial of service (DoS) condition.

Due to a design error in the clean-up code following certain types of failed queries, it is possible to cause the server to call the free() function on an address obtained from uninitialized memory. This can result in an invalid memory reference leading to denial of service.

III. ANALYSIS

Exploitation of this vulnerability allows remote attackers to cause a denial of service against the affected server, 'ns-slapd'.

In some situations it may be possible to put information from the remote attacker in the memory range being accessed which may allow execution of code, however this has not yet been demonstrated.

IV. DETECTION

iDefense has confirmed Sun Java System Directory Server 5.2 Directory Server 5.2 2005Q4 is affected by this vulnerability. Previous versions are also suspected to be vulnerable.

V. WORKAROUND

Restrict remote access at the network boundary, unless remote parties require service. Access to the affected host should be filtered at the network boundary if global accessibility is not required. Restricting access to only trusted hosts and networks may reduce the likelihood of exploitation.

VI. VENDOR RESPONSE

Sun Microsystems Inc. has addressed this issue in Sun Java System Directory Server 5.2 Patch5. For more information see Sun Alert ID 102853 by visiting the URL shown below.

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102853-1>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2006-4175 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

08/16/2006 Initial vendor notification
08/21/2006 Initial vendor response
03/23/2007 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research
<http://labs.odefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events
<http://labs.odefense.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.