

[VulnWatch] iDefense Security Advisory 05.02.07: LiveData Protocol Server Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-05/msg00002.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Wed, 02 May 2007 14:53:22 -0400
-

LiveData Protocol Server Heap Overflow Vulnerability

iDefense Security Advisory 05.02.07

<http://labs.iddefense.com/intelligence/vulnerabilities/>

May 02, 2007

I. BACKGROUND

LiveData is a provider of real-time data acquisition and processing software. LiveData Protocol Server is used in SCADA environments to record and transmit data to other control points in process control networks. The LiveData server includes a HTTP server that offers a SOAP interface to the product. More information is available at the vendor's web site at the following URL.

<http://www.livedata.com/>

II. DESCRIPTION

Remote exploitation of a heap overflow vulnerability within LiveData's Protocol Server could allow an attacker to cause the service to crash or potentially execute arbitrary code with SYSTEM privileges.

The vulnerability specifically exists due to the the handling of requests for WSDL files. By supplying a specially crafted request to the service on port 8080, an attacker is able to supply a negative length value to a strncpy call.

This value is interpreted by strncpy as a very large positive value. As a result, a memory access violation occurs when attempting to write data past the end of the heap memory segment.

III. ANALYSIS

Exploitation allows an attacker to crash the LiveDataServer service or

potentially execute arbitrary code.

Arbitrary code execution would depend on overwriting heap data that is used within a different thread. A race condition would have to exist where the flow of execution would be diverted before the application terminated from the memory access violation.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability in LiveData Protocol Server version 5.00.045 which was the current release as of September 13th 2006.

V. WORKAROUND

In order to mitigate potential exploitation, iDefense recommends blocking access to port 8080 by using a firewall.

VI. VENDOR RESPONSE

LiveData has addressed this vulnerability with updated versions of their software. The following versions are reported to be fixed.

RTI update 500062

Protocol Server update 500062

Maintenance Server update 500062

VII. CVE INFORMATION

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

VIII. DISCLOSURE TIMELINE

01/02/2007 Initial vendor notification

01/03/2007 Initial vendor response

05/02/2007 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@xxxxxxxxxxxx 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.