

[NEWS] LiveData Protocol Server Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 7 May 2007 12:38:19 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

LiveData Protocol Server Heap Overflow Vulnerability

SUMMARY

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

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.

DETAILS

Vulnerable Systems:

* LiveData Protocol Server version 5.00.045 which was the current release as of September 13th 2006.

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

[NEWS] LiveData Protocol Server Heap Overflow Vulnerability

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.

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.

Workaround:

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

Vendor Status:

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

Disclosure Timeline:

- * 01/02/2007 Initial vendor notification
- * 01/03/2007 Initial vendor response
- * 05/02/2007 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=523>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=523>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

[NEWS] LiveData Protocol Server Heap Overflow Vulnerability

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.