

[UNIX] MySQL MaxDB Web Agent Multiple DoS Vulnerabilities (sapdbwa_GetUserData)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:23:11 +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>

MySQL MaxDB Web Agent Multiple DoS Vulnerabilities (sapdbwa_GetUserData)

SUMMARY

<<http://www.mysql.com/products/maxdb/>> MaxDB by MySQL is "a re-branded and enhanced version of SAP DB, SAP AG's open source database. MaxDB is a heavy-duty, SAP-certified open source database that offers high availability, scalability and a comprehensive feature set. MaxDB complements the MySQL database server, targeted for large mySAP ERP environments and other applications that require maximum enterprise-level database functionality".

Two remotely exploitable denial of service conditions have been found to exist in MySQL MaxDB and SAP DB Web Agent products.

DETAILS

Vulnerable Systems:

* MySQL MaxDB version 7.5.0.20 and prior

The first vulnerability specifically exists due to a NULL pointer dereference in the `sapdbwa_GetUserData()` function. A remote attacker can request the WebDAV handler code with invalid parameters to cause a NULL

Securiteam: [UNIX] MySQL MaxDB Web Agent Multiple DoS Vulnerabilities (sapdbwa_GetUserData)

pointer dereference resulting in a crash of SAP DB Web Agent.

The second vulnerability is due to insufficient handling of malformed HTTP headers. A remote attacker can submit a HTTP request with invalid headers to cause a denial of service.

Analysis:

A remote attacker can send simple HTTP requests to cause MaxDB Web Agent to crash.

Workaround:

Employ firewalls, access control lists or other TCP/UDP restriction mechanisms to limit access to administrative systems and services.

Vendor response:

The vulnerability has been addressed in MaxDB 7.5.00.21.

Updated binaries (version 7.5.00.23) are available from:

<<http://dev.mysql.com/downloads/maxdb/7.5.00.html>>
<http://dev.mysql.com/downloads/maxdb/7.5.00.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0081>>
CAN-2005-0081
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0082>>
CAN-2005-0082

Disclosure Timeline:

08/20/2004 – Initial vendor notification
08/24/2004 – Initial vendor response
01/19/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> IDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=187&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=187&type=vulnerabilities>

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.