

[UNIX] ADOdb SQL Injection and PHP Code Execution Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00032.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 11 Jan 2006 09:52:52 +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>

ADODB SQL Injection and PHP Code Execution Vulnerabilities

SUMMARY

" <<http://adodb.sourceforge.net/>> ADOdb is a database abstraction library for PHP."

Two vulnerabilities in ADOdb can be exploited by malicious attackers to disclose system information, execute arbitrary PHP code, execute arbitrary SQL code, and potentially compromise a vulnerable system.

DETAILS

Vulnerable Systems:

- * ADOdb version 4.66
- * ADOdb version 4.68

Immune Systems:

- * ADOdb version 4.70

SQL Injection:

The problem is caused due to the presence of the insecure "server.php" test script. This can be exploited to execute arbitrary SQL code with full

[UNIX] ADOdb SQL Injection and PHP Code Execution Vulnerabilities

MySQL database privileges via the "sql" parameter.

Proof of Concept:

[http://\[victim\]/server.php?sql=SELECT '\[content\]' INTO OUTFILE '\[file\]'](http://[victim]/server.php?sql=SELECT '[content]' INTO OUTFILE '[file]')

This can further be exploited to create an arbitrary PHP script in a directory inside the web root writable by the MySQL user. Successful exploitation requires that the MySQL password for the root user is empty and that the affected script is placed accessible inside the web root.

Code Execution:

The problem is caused due to the presence of the insecure "tests/tmssql.php" test script. This can be exploited to call an arbitrary PHP function via the "do" parameter.

Proof of Concept:

[http://\[victim\]/tests/tmssql.php?do=phpinfo](http://[victim]/tests/tmssql.php?do=phpinfo)

Successful exploitation requires that the affected script is placed accessible inside the web root.

Disclosure Timeline:

- 30/12/2005 – Initial vendor notification.
- 03/01/2006 – Other affected vendors notified.
- 05/01/2006 – Initial vendor reply.
- 08/01/2006 – New version of ADOdb released.
- 09/01/2006 – Public disclosure.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vuln@xxxxxxxxxxxx>> Secunia Research.

The original article can be found at:

<http://secunia.com/secunia_research/2005-64/advisory/>
http://secunia.com/secunia_research/2005-64/advisory/

=====

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@xxxxxxxxxxxx

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

=====

=====

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.

- Prev by Date: [*\[TOOL\] TCP/UDP Protocol Fuzzer \(CIRT.DK\)*](#)
- Next by Date: [*\[NT\] Visual Studio Code Execution \(Exploit\)*](#)
- Previous by thread: [*\[TOOL\] TCP/UDP Protocol Fuzzer \(CIRT.DK\)*](#)
- Next by thread: [*\[NT\] Visual Studio Code Execution \(Exploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)