

[NEWS] Multiple Issues with SAP DB Web-tools

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/17/03

To: list@securiteam.com

Date: 17 Nov 2003 18:43:27 +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>

Multiple Issues with SAP DB Web-tools

SUMMARY

<<http://www.sapdb.org>> SAP's open source database server is a project sponsored by SAP AG. The database server allows for a fast, flexible, high performance and easily administered deployment of an enterprise level database solution. In addition to the base package, the SAP DB project also ships a 'web-tools' solution that can either be integrated into existing web server solutions (i.e. IIS or iPlanet) or alternatively run its own native web server.

There exist a number of vulnerabilities in the native web server solution that could enable an attacker to perform a number of operations against the host in question and/or other database servers that the web server communicates with.

The vulnerabilities outlined in the advisory below are examples of why the default functionality should be evaluated in terms of new vulnerabilities and risks they may introduce before being deployed in a production environment.

DETAILS

Vulnerable systems:

Securiteam: [NEWS] Multiple Issues with SAP DB Web-tools

* SAP DB versions prior to 7.4.03.30

Immune systems:

* SAP DB version 7.4.03.30

Directory Traversal

Within the web-tools component exists a directory traversal vulnerability that enables an attacker to retrieve any file off the host drive on which the web-tools component resides upon. Also it should be noted that by default the SAP web server's runs as Local SYSTEM by default on Windows NT/2000/XP Platforms so all files are retrievable.

During a request no URL decoding occurs, simply put the request is passed to the 'sqlfopenc' function which checks the file requested does indeed exist. If it is then the entire URI is simply supplied to the 'FileFound' function which in turn returns the file to the user. Contained below is the code, which is at fault:

```
-----[Start: sqlfopenc Function]
sqlfopenc (path, SP5VF_BINARY, SP5VF_READ, SP5BK_BUFFERED,
          &fin, &err);
if (err.sp5fe_result != vf_ok)
    rtc = FileNotFound(req->uri, host, port, as, rep);
else
{
    rtc = FileFound(path, as, req, rep, fin);
    sqlfclosec (fin, SP5VF_CLOSE_NORMAL, &err);
}
-----[End: sqlfopenc Function]
```

To successfully exploit this vulnerability an attacker simply needs to perform a tried and tested double-dot attack to retrieve the file of choice (i.e. '<http://127.0.0.1:85/../../../../../../../../boot.ini>').

Web Agent Administration open by default

By default any user who has access to the SAP DB web-tools can access the Web Agent Administration pages without prior authentication by simply requesting a URL similar to '<http://127.0.0.1:85/waadmin.wa>'.

From within the WAA an attacker can configure a large range of options such as but not limited to:

- Global Settings

Configure such items as the SAP DB WWW document root.

- Services

Configure a URL which will call a certain function out of a library of choice (i.e. from DLL such as Kernel32 on Windows)

- COM Services

Configure a service that can call any class ID which is installed on the

local machine.

Web Agent Administration service contains buffer overflow

In addition the Web Agent Administration pages contain at least one buffer overflow as well as the vulnerabilities mentioned above. By entering a overly long URL such as:

<http://127.0.0.1:85/wadmin.wa?Service=Service&Name=AAAAAA...>

An attacker can cause a buffer overflow to occur within, from @stake's testing we were able to overwrite EIP (IA32) with EBX pointing to our malicious buffer. If successfully exploited an attacker can obtain 'SYSTEM' level access on Windows.

Default services within Web Agent / WAECHO buffer overflow

Within the default installation of the SAP DB web-tools contains a number of default services. These services can be used by an attacker to launch a mired of attacks against either the host upon which they are installed or against other database servers with which the SAP DB web-agent host has connectivity to.

– waecho

Within the SAP DB WWW (SAP Native, IIS or NES) there is a default service called waecho which is requested as via a URL similar to:

<http://127.0.0.1:85/waecho>

In response it simply spits out a number of variables the first of which is requestURI an example of which is contained below:

requestURI = /waecho/

By passing an overly long string on the URL such as:

<http://127.0.0.1:85/waecho/AAAAAAA...>

Will cause a buffer overflow to occur, EIP is over written (IA32) and EDI points to about 120 bytes before our buffer. If successfully exploited an attacker can execute code as 'SYSTEM' on Windows platforms. The offending library (waecho.dll on Windows or vwd83echo.c within the source tree) contains the following offending code:

```
-----[Start: wd83ShowVal function from vwd83echo.c]
void wd83ShowVal( sapdbwa_HttpReplyP rep, const char *name,
                  const char *val )
{
char textBuffer[1024];
if (val != NULL) {
    sprintf( textBuffer, name, val );
} else {
    sprintf( textBuffer, name, "NULL" );
}; /* else */
strcat( textBuffer, "\n" );
sapdbwa_SendBody( rep, textBuffer, strlen( textBuffer
    ) );
}
```

Securiteam: [NEWS] Multiple Issues with SAP DB Web-tools

```
} /* wd83ShowVal */
```

-----[End: wd83ShowVal function from vwd83echo.c]

– websql / webdbm

Another two default services are the 'websql' and 'webdbm' which allows a remote user to either connect to and execute queries or manage a database if the database name, username and password are known. The issue here is that this can be utilized potentially by someone outside of the enterprise to connect to other databases which are not to be publicly accessible via web applications.

Web SQL Interface: <http://127.0.0.1:85/websql>

Web Database Manager: <http://127.0.0.1:85/webdbm>

Web Database Manager session ID generation

Within the Web Database Manager there is the possibility of performing a number of actions. To keep track of the session these an ID is generated, but not kept in cookie as per the norm. Instead these session ID's are stored in the URL. The manner in which these session ID's are generated can be considered unsafe, below is sample which @stake took:

<http://127.0.0.1:85/webdbm/014000000000>

<http://127.0.0.1:85/webdbm/015000000000>

<http://127.0.0.1:85/webdbm/016000000000>

<http://127.0.0.1:85/webdbm/017000000000>

<http://127.0.0.1:85/webdbm/018000000000>

<http://127.0.0.1:85/webdbm/019000000000>

<http://127.0.0.1:85/webdbm/020000000000>

As you can see these session ID's simply increment by 1000000000 each time.

Vendor Response:

@stake has contacted the vendor multiple times since August 2002 until May 2003 below is the time line of the communication:

29-Aug-2002: @stake confirms e-mail contact details of for security issues

29-Aug-2002: @stake confirms SAP doesn't support encrypted e-mail

29-Aug-2002: SAP confirms they have received it and passed it on to the developer who wrote the code.

03-Dec-2002: @stake gets e-mail from SAP concerning another security issue they have resolved and a link to a URL.

Dec-2002: @stake asks for status update from SAP.

Jan-2003: @stake asks for status update from SAP.

24-Jan-2003: Send e-mail to SAP asking if they received @stake's communications.

24-Jan-2003: @stake gets confirmation e-mail back stating they are still trying to get a timeline together.

Mar-2003: @stake asks for time line on when these issues will be fixed.

31-Mar-2003: Get e-mail saying the priority for removing these flaws has been shifted down again.

Securiteam: [NEWS] Multiple Issues with SAP DB Web-tools

18-Apr-2003: @stake sends e-mail to SAP informing them of our advisory policy and it has been nearly 8 months since initial communication on the vulnerabilities. @stake informs SAP of four (4) weeks notice until we release unless advised of an update schedule and that @stake is happy to delay release until a fix is available if they can supply a solid date/time frame by which the issues will be resolved.

21-Apr-2003: Receive confirmation e-mail that my message has been passed on to the people developing the project plan. In addition @stake is informed they have been notified of all of @stake's past e-mails.

18-May-2003: @stake e-mails contact saying no response has been heard.

??-May-2003: Inform vendor we are releasing advisory and supply final @stake draft with time line in.

??-Jun-2003: SAP reestablish contact

29-Aug-2003: 1 year since vendor notified

07-Nov-2003: SAP releases version 7.4.03.30 which fixes all of the @stake reported vulnerabilities.

17-Nov-2003: Release

Recommendation:

If the SAP DB WWW service is not required then it should be removed or disabled on the host in question. If it is required, enterprises should deploy vendor patches for the above vulnerabilities. Version 7.4.03.30 contains fixes for all vulnerabilities.

In addition, enterprises should look to remove all default services if not required in production systems or adequately protect those that are required.

ADDITIONAL INFORMATION

The original advisory is available from:

<<http://www.atstake.com/research/advisories/2003/a111703-2.txt>>
<http://www.atstake.com/research/advisories/2003/a111703-2.txt>.

The information has been provided by Ollie Whitehouse of <<mailto:advisories@atstake.com>> @stake Advisories.

=====

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.