

[NT] Multiple Vulnerabilities in Comersus BackOffice Lite

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0092.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:31:33 +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 Vulnerabilities in Comersus BackOffice Lite

SUMMARY

<<http://www.comersus.com/index.html>> Comersus ASP shopping cart is "a set of ASP scripts creating an online shopping cart. It works on a database of your own choosing, default is Microsoft Access, and includes online administration tools".

Multiple security vulnerabilities have been discovered in the product allowing an attacker: complete access over the product by accessing a specific page, to inject arbitrary SQL statements into the program's existing SQL statements and to cause cross site scripting vulnerabilities.

DETAILS

Vulnerable Systems:

- * Comersus BackOffice Lite version 6.0
- * Comersus BackOffice Lite version 6.01

Immune Systems:

- * Comersus BackOffice Lite version 6.02

Securiteam: [NT] Multiple Vulnerabilities in Comersus BackOffice Lite

Administrative Privileges Bypassing:

The /backofficelite/comersus_backoffice_install10.asp file is the last step in the installation sequence of the ASP web Cart. One doesn't have to be a shopping cart administrator to execute this file. Besides setting the value of some variables, it also contains the following code:

```
session("admin")=1
```

registering the current session as having administrator rights on the shopping cart software.

Therefore, by running this script one gives oneself full right to all the scripts, including scripts to enter any SQL command, decrypt passwords, etc...

Workaround:

Deleting the file after installation process has been completed.

SQL Injection in Referer String:

If the option pIndexVisitsCounter is set to -1 (this is not done by default), the /store/default.asp script will add a line to the database:

```
mySQL="INSERT INTO visits (userId, referrer, visitDate,
visitTime, idStore)
VALUES
('"&pUserId&"','"&pReferrer&"','"&pVisitDate&"','"&pVisitTime&"','
&pIdStore& ")"
```

Interesting here is the pReferrer variable, which is loaded as follows:

```
pReferrer = request.ServerVariables("HTTP_REFERER")
```

No further data validation is done on the MySQL string before it is sent to the database for processing. This allows the attacker to create his own HTTP GET request and entering SQL code into the referer field, e.g.:

```
GET /comersus/store/default.asp HTTP/1.1
Referer: <SQLCODE HERE>
```

Workaround:

Disable visitor logging (pIndexVisitsCounter = 0).

Cross Site Scripting:

The following two files: comersus_supportError.asp and comersus_backofficelite_supportError.asp are prone to a cross site scripting vulnerability.

Example:

[http://host/comersus/backofficelite/comersus_supportError.asp?error=>alert\('hi%20mum'\);</script>](http://host/comersus/backofficelite/comersus_supportError.asp?error=>alert('hi%20mum');</script>)

Vendor response:

The vendor has issued an advisory that explains what vulnerable sites should do to redeem these vulnerabilities:

<http://www.comersus.org/forum/displayMessage.asp?mid=32753>
<http://www.comersus.org/forum/displayMessage.asp?mid=32753>

Securiteam: [NT] Multiple Vulnerabilities in Comersus BackOffice Lite

ADDITIONAL INFORMATION

The information has been provided by <mailto:beltech2bugtraq@hotmail.com>
raf somers.

=====

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.