

[NT] Spider Sales Shopping Cart Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0028.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/10/04

To: list@securiteam.com

Date: 10 Mar 2004 18:15:42 +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>

Spider Sales Shopping Cart Multiple Vulnerabilities

SUMMARY

" <<http://www.spidersales.com>> Spider Sales is a powerful shopping cart solution designed for small, medium or large enterprises who want to sale their products on the Internet market. You can use it to build any kind of Internet shop and virtually sell anything". Vulnerabilities in Spider Sales Shopping Cart allow a malicious user to decrypt protected information without the proper authentication. A malicious user can also run arbitrary SQL commands on the server.

DETAILS

Incorrect use of cryptography:

Spider Sales shopping cart software uses RSA cryptosystem to encrypt sensitive data before storing it in a database. The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Please read

<<http://www.rsasecurity.com/rsalabs/faq/3-1-1.html>>

<http://www.rsasecurity.com/rsalabs/faq/3-1-1.html> for more information about RSA cryptosystem. In the Spider Sales shopping cart software the maximum length of the modulus n is equal to 20 bits and don't have minimum

Securiteam: [NT] Spider Sales Shopping Cart Multiple Vulnerabilities

length limit, so it is easy for attacker to factor n into p and q and obtain the private key d. Moreover, the private key is stored in the same database and in the same table where a public key is. So an attacker can decrypt any protected information if he gains access to store's database.

SQL Injection:

Substantial number of scripts in Spider Sales software don't filter 'userId' parameter, which can be used by attacker for modifying SQL query and perform some of SQL injection attacks.

Successful exploitation of this vulnerability could allow an attacker to gain access to Spider Sales administrator interface and read any information from store's database (i.e. customers private data). Also an attacker could execute commands using xp_cmdshell function.

Proof of concept:

The following request executes dir c: command and saves result in c:\inetpub\wwwroot\dir.txt file

[http://\[target\]/viewCart.asp?userID=2893225125722634';exec%20master..xp_cmdshell%20'dir%20c:%20>%20c:\inetpub\wwwroot\dir.txt'](http://[target]/viewCart.asp?userID=2893225125722634';exec%20master..xp_cmdshell%20'dir%20c:%20>%20c:\inetpub\wwwroot\dir.txt')

Vendor Status:

S-Quadra alerted Spider Sales development team to these issues on 25 Feb 2004. No response has been received. No fix information has been provided.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:research@s-quadra.com>>
S-Quadra Security Research.

=====

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.