

[UNIX] MaxWebPortal Cross Site Scripting and SQL Injection Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0026.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/11/04

To: list@securiteam.com

Date: 11 Feb 2004 16:53:54 +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>

MaxWebPortal Cross Site Scripting and SQL Injection Vulnerabilities

SUMMARY

" <<http://www.maxwebportal.com>> MaxWebPortal is a web portal and online community system which includes advanced features such as web-based administration, poll, private/public events calendar, user customizable color themes, classifieds, user control panel, online pager, link, file, article, picture managers and much more."

MaxWebPortal contains multiple vulnerabilities which allow cross-site scripting, SQL injection and Avatar ScriptCode injection.

DETAILS

Vulnerable Systems:

* MaxWebPortal version 1.31

Immune Systems:

* MaxWebPortal version 1.32

Cross-site Scripting

Cross-site scripting is possible from within 'dl_showall.asp' due to

Securiteam: [UNIX] MaxWebPortal Cross Site Scripting and SQL Injection Vulnerabilities

insufficient filtering of the 'sub_name' parameter as well as the 'SendTo' parameter in Personal Messages that allows arbitrary code execution on the client-side browser. Another cross-site scripting vulnerability exists in the 'down.asp' script. Due to insufficient filtering of the HTTP_REFERER header an attacker can forge headers which contain arbitrary HTML and script code.

Example:

```
< A HREF="< % =Request.ServerVariables("HTTP_REFERER") %>">Back< /FONT>< /A>< /P>
```

SQL Injection

SQL injection is possible through the 'SendTo' parameter in Personal Messages due to insufficient sanitation. It can then lead to information disclosure from the database.

Avatar ScriptCode Injection

In the 'register' form there is no input validation when inserting an image name of an Avatar into the database. This can be exploited by a malicious user to inject arbitrary HTML or ScriptCode instead of an Avatar. Such an attack can be used for example to steal another user's cookies if the user visits a page where the attacker user's Avatar image would have been displayed.

Example:

```
< select name="Avatar_URL" size="4" onChange ="if (CheckNav(3.0,4.0))
URL.src=form.Avatar_URL.options[form.Avatar_URL.options.selectedIndex].value;">
< option value="javascr!pt:alert(document.cookie)">POC-Avatar< /option><
/select>
```

NOTE: In the above example, the word 'javascript' has been replaced with 'javascr!pt'.

Vendor Status:

The vendor has been notified and released a newer version. Upgrade to version 1.32.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mantra@gulo.org> Manuel Lopez.

=====

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

=====

=====

Securiteam: [UNIX] MaxWebPortal Cross Site Scripting and SQL Injection Vulnerabilities

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.