

[UNIX] Multiple Vulnerabilities in Phorum (common.php, common.php, login.php, register.php)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0025.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/07/04

To: list@securiteam.com

Date: 7 Jan 2004 16:30:35 +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 Phorum (common.php, common.php, login.php,
register.php)

SUMMARY

<<http://www.phorum.org/>> Phorum is "an Open Source web based discussion software application written in PHP". Multiple security flaws in the product allow remote users to cause SQL injection vulnerability, and multiple cross-site scripting vulnerabilities.

DETAILS

Vulnerable systems:

- * Phorum version 3.4.5 and prior

Immune systems:

- * Phorum version 3.4.6
- * Phorum version 5.0.2 alpha

Phorum is vulnerable to cross-site scripting and SQL injection bugs that could allow for the remote compromise of any server running the affected software.

Vulnerability #1:

An XSS vulnerability exists in the script 'common.php' that allows arbitrary code execution on the client-side browser. Ironically, this vulnerability is in the 'phorum_check_xss()' function. The vulnerable code is below:

```
if(!is_array($value) && $key!="body" && $key!="subject" && $key!="hide" && strpos($value, "< script")){ echo "script detected in $key";
```

By sending a HTTP/POST variable to any Phorum script, an attacker could craft the key of the variable into an XSS attack, providing the value of the variable contains the string "< script".

Vulnerability #2:

Another XSS vulnerability exists in the script 'profile.php'. This vulnerability exists via insufficient sanitization of the variable 'EditError'. If a user is logged on, an attacker could use this vulnerability to include arbitrary code on the user's browser.

NOTE: Phorum (common.php) does checks for '< script>' tags, however XSS attacks are not limited to just the < script> tags! An attacker could use many forms of XSS (such as < iframe>) to launch attacks upon users.

Vulnerability #3:

Once again, there is an XSS vulnerability in the script 'login.php' that may allow attackers to execute arbitrary code in the users' browser. This exploit is due to (again) the 'Error' variable not being sanitized correctly.

Vulnerability #4:

A SQL Injection vulnerability exists in the script 'register.php' in the field 'hide_email'. This vulnerability could lead to the execution of SQL commands inside the script.

Vendor status:

Phorum has released Phorum v3.4.6 as a response to this advisory. Please patch your vulnerable software ASAP.

ADDITIONAL INFORMATION

The information has been provided by <mailto:enune@fribble.net> Calum Power.

=====

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.