

[Full-disclosure] iDEFENSE Security Advisory 11.10.05: Tikiwiki tiki-user_preferences Command Injection Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-11/0291.html>

From: iDEFENSE Labs (labs-no-reply_at_idefense.com)

Date: 11/11/05

To: <bugtraq@securityfocus.com>, <vulnwatch@vulnwatch.org>, <full-disclosure@lists.grok.org.uk>

Date: Thu, 10 Nov 2005 19:06:37 -0500

Tikiwiki tiki-user_preferences Command Injection Vulnerability

iDEFENSE Security Advisory 11.10.05

www.idefense.com/application/poi/display?id=335&type=vulnerabilities

November 10, 2005

I. BACKGROUND

Tikiwiki Community Portal is a full featured, freely available, Wiki/CMS/Groupware system written in PHP. More information is available at:

<http://tikiwiki.org/>

II. DESCRIPTION

Remote exploitation of an input validation vulnerability in Tikiwiki could allow attackers to gain access to arbitrary files on the vulnerable system and execute arbitrary code under the privileges of the underlying web-server.

The problem specifically exists in the following snippet of code from `tiki-user_preferences.php`:

```
if (isset($_REQUEST["prefs"])) {  
...  
    if ($change_language == 'y') {  
        if (isset($_REQUEST["language"])) {  
            $tikilib->set_user_preference($userwatch, 'language', \  
                $_REQUEST["language"]);  
  
            $smarty->assign('language', $_REQUEST["language"]);  
            include ('lang/' . $_REQUEST["language"] . \  
                '/language.php');
```

```
}  
}
```

No sanity checking is done on the 'language' parameter prior to utilizing it in a call to the PHP function include(). By specifying a path with directory traversal modifiers, an attacker can request an arbitrary file to load and render on the screen.

III. ANALYSIS

Exploitation could allow authenticated remote attackers to access arbitrary files on the vulnerable system with the privileges of the underlying web-server. If external database access is allowed, exploitation can result in a full database compromise since database credentials are easily exposed through this vulnerability.

Exploitation can result in arbitrary command execution with the privileges of the underlying targeted web server. This is possible because attackers can generate request URLs with arbitrary script directives that are recorded in the web server log files. Attackers can then utilize the path to the poisoned log file in the file inclusion, resulting in the directives being parsed and executed.

IV. DETECTION

iDEFENSE has confirmed the existence of this issue in Tikiwiki versions 1.8.4 and 1.8.5. It is suspected that earlier versions are vulnerable as well.

V. WORKAROUND

Restrict anonymous access to Tikiwiki. If remote database connectivity is not required, configure the underlying database server to bind to localhost only or firewall the listening port to accept trusted hosts only. Restrict read access of log files from the web server user.

VI. VENDOR RESPONSE

This vulnerability has been addressed in Tikiwiki 1.9.1 which is available for download at:

<http://tikiwiki.org/tiki-index.php?page=Download>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2005-1925 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

06/07/2005 Initial vendor notification
08/21/2005 Initial vendor response
11/10/2005 Public disclosure

IX. CREDIT

This vulnerability was discovered by both Maciej Piotr Falkiewicz (fingerout[at]gmail[dot]com) and an anonymous contributor.

Get paid for vulnerability research
<http://www.idefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events
<http://labs.idefense.com>

X. LEGAL NOTICES

Copyright C 2005 iDEFENSE, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDEFENSE. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email customerservice@idefense.com for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>