

[UNIX] dotproject Remote File Access Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0080.html>

From: support@securiteam.com

Date: 01/30/03

From: support@securiteam.com

To: list@securiteam.com

Date: 30 Jan 2003 11:21:43 +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

dotproject Remote File Access Vulnerability

SUMMARY

dotproject is a PHP+MySQL beta level web based project management and tracking tool that dotmarketing started in Dec. 2000. A vulnerability exists in a file named core.php that is found in the /locale/ directory. Because there is neither .htaccess set on this directory nor any security check in core.php, an attacker may call it directly and read local files with web server permissions.

DETAILS

Here is the code of core.php:

```
<?php
ob_start();
@readfile( "$root_dir/locales/$AppUI->user_locale/common.inc" );
@readfile( "$root_dir/locales/$AppUI->user_locale/$m.inc" );
.
```

We can see that \$root_dir is never defined before and may be injected if globals are on. An attacker may type in the browser the following URI: http://victim/dotproject/locales/core.php?root_dir=/file_or_dir_path/%00

Securiteam: [UNIX] dotproject Remote File Access Vulnerability

Here %00 just ignores everything that comes after it so that the attack may be able to read any file 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 /locale/ 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

=====

=====

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.